ВЕРИФИКАЦИЯ ПРОТОКОЛОВ БЕЗОПАСНОСТИ НА ОСНОВЕ КОМБИНИРОВАННОГО ИСПОЛЬЗОВАНИЯ СУЩЕСТВУЮЩИХ МЕТОДОВ И СРЕДСТВ

КОТЕНКО И.В., РЕЗНИК С.А., ШОРОВ А.В.

УДК 004.42:004.94:004.7

Котенко И.В., Резник С.А., Шоров А.В. **Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств.**

Аннотация. В настоящей статье анализируются существующие подходы к верификации протоколов безопасности и демонстрируется невозможность полноценной верификации протоколов безопасности в рамках только одного из подходов. Для решения данной задачи предлагается комбинированный подход к верификации, основанный на объединении сильных сторон существующих методов и средств.

Ключевые слова: протоколы безопасности, формальные методы, верификация, проверка на модели, доказательство теорем.

Kotenko I.V., Reznik S.A., Shorov A.V. **Security protocols verification combining existing approaches and tools.**

Abstract. This paper evaluates existing approaches to the security protocols verification and explains why it is impossible to thoroughly verify security protocols using only one of them. To solve this problem combined verification approach which is based on the assembly of strong sides specific for different existing approaches and tools is suggested.

Keywords: security protocols, formal methods, verification, model checking, theorem proving.

1. Введение. Процесс разработки протоколов безопасности включает в себя проверку (верификацию) того, что они обеспечивают требуемые свойства безопасности. Такая проверка включает в себя:

1) проверку надежности криптографических примитивов,

2) проверку стойкости протокола безопасности к атакам в предположении о надежности криптографических примитивов, на которые он опирается.

Второй аспект верификации и является предметом настоящей работы.

Для решения такой задачи был разработан целый ряд подходов, основанных как на методах проверки на модели (*model checking*), так и на доказательстве теорем (*theorem proving*). Однако, как видно из представленного в данной работе анализа, каждый из существующих подходов имеет, помимо достоинств, существенные недостатки.

Это обстоятельство делает актуальной проблему разработки методологии верификации, основанной на комбинировании существующих методов и средств, подход к решению которой предлагается в настоящей работе.

В настоящей момент опубликовано несколько работ, посвящен-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ных анализу подходов к верификации протоколов безопасности (например [21, 10, 15, 22, 4] и др.). Обзор [21] подготовлен достаточно давно и не отражает существующего многообразия подходов. Анализ публикаций [10], посвященных протоколам аутентификации, включает главу, в которой говорится о работах по верификации протоколов, но данная работа также не отражает современные работы. Анализ, рассмотренный в [4], представляется наиболее актуальным из существующих обзоров по различным подходам к верификации протоколов. Однако данная работа в основном посвящена изложению существа данных подходов и не предлагает способов комбинирования существующих средств верификации.

Настоящая работа содержит анализ последних исследований в данной области в аспекте их использования для формирования комбинированного подхода к верификации, основанного на объединении сильных сторон существующих подходов.

Статья структурирована следующим образом.

Раздел 2 содержит общий обзор работ в области верификации протоколов безопасности.

В разделе 3 определяются критерии, на основании которых можно делать выбор в пользу того или иного подхода или средства верификации.

В разделе 4 рассматриваются имеющиеся подходы и реализующие их средства верификации, базирующиеся на использовании методов проверки на модели и логического вывода.

Раздел 5 посвящен обоснованию недостаточности отдельно взятого подхода для полноценной верификации протоколов безопасности, в нем предлагается комбинированный подход к верификации протоколов безопасности и описывается его использование для верификации EnTrusting-протокола, применяемого для защиты программного обеспечения на основе принципов удаленного доверия.

В заключении подводятся итоги проделанной работы и определяются направления дальнейших исследований.

2. Общая характеристика базовых работ в области верификации протоколов безопасности. Статья [18] во многом определила основы формальной верификации протоколов. Данная работа обосновывает необходимость формальной верификации протоколов безопасности, а протокол Нидхема—Шрёдера с открытыми ключами, рассмотренный в ней, является примером, демонстрирующим возможности средств верификации.

В [13] показана алгоритмическая неразрешимость задачи верифи-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

кации протоколов в общем виде. Этот результат важен для понимания ограниченности возможностей существующих подходов, которые рассматриваются ниже.

Подход к обнаружению атак на протоколы безопасности на основе моделирования протокола с помощью формализма CSP (Communicating Sequential Processes) представлен в [19]. Развитие идей моделирования на основе CSP представлено в [20].

Работы [23] и [25] описывают верификацию протоколов NSPK и SSL с помощью средства проверки на модели Murphi.

В [17] рассматривается применение средства проверки на модели SPIN для верификации протокола X.509.

Использование средства вероятностной проверки на модели PRISM для оценки вероятностных свойств протоколов представлено в [31] и [27].

Применение сетей Петри для анализа протоколов безопасности представлено в работе [26].

В [14] рассматривается язык описания протоколов CAPLS (Common Authentication Protocol Specification Language), предназначенный для универсального описания протоколов безопасности (для использования с разными средствами верификации), а [24] предлагает подход к верификации протоколов, основанный на разрешении ограничений с использованием CAPSL в качестве языка описания протоколов.

Работы [7] и [5] описывают использование Пи-исчисления и дизъюнктов Хорна для верификации протоколов с помощью средства ProVerif. Данный подход позволяет верифицировать протоколы в случае неограниченного количества сообщений и сеансов. Достигается это за счет потери точности верификации — возможны ложные обнаружения атак (варианты ложной корректности невозможны).

Кроме того, в рамках данного подхода можно проверить свойство строгой секретности (невозможность обнаружения злоумышленником факта изменения данных, а не только самих данных, как в случае классической секретности).

В рамках проекта AVISPA, описанного в [32], предпринята попытка создания универсального средства верификации, позволяющего предоставлять описание протокола с помощью универсального языка HLPLS (High Level Protocol Specification Language) и после преобразования его в промежуточное представление IF (Intermediate Format) вызывать одно из нескольких средств верификации. В рамках проекта AVISPA предоставляются четыре таких средства (OFMC; CL-AtSe;

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

SATMC; TA4SP), а также существует возможность разрабатывать другие средства верификации, воспринимающие промежуточное представление IF в качестве входного языка.

Работа [8] описывает подход, реализованный в верификаторе OFMC (On the Fly Model Checker). Этот подход основывается на представлении множества состояний в виде дерева, корнем которого является начальное состояние, а узлы нижнего уровня для каждого узла дерева определяются как состояния, в которые система может перейти за один шаг. Для представления такого дерева используется механизм отложенных вычислений, а в ходе анализа выбирается конечное подмножество состояний, что позволяет завершить анализ за конечное время.

В [30] описывается метод верификации, используемый компоненте CL-AtSe (Constraint Logic based Model-Checking of Security Protocols). Он основан на логике ограничений и во многом схож с подходом, используемым в CAPSL.

Метод верификации, используемый в компоненте SATMC (SAT-based Model Checker), представлен в [11]. Он основан на сведении задачи выявления уязвимости протокола по отношению к атакам конечной длины к задаче разрешимости пропозициональной формулы, с помощью подходов, применяемых в области SAT-разрешимости.

В [28] рассматривается подход, использованный в верификаторе TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols). Он основан на перезаписи термов и аппроксимации, позволяющей выявлять уязвимость протокола в случае бесконечного количества сеансов.

В [12] предлагается метод верификации, основанный на уточнении шаблонов. Он гарантирует ответ в случае бесконечного количества сеансов. Этим ответом может быть либо доказательство того, что протокол не обладает необходимым свойством, либо доказательство, что он обладает им в бесконечном случае, либо доказательство для конечного случая.

Еще один метод верификации протоколов безопасности основан на применении общих методов автоматизированного доказательства теорем. В частности, средство Isabelle, общие принципы работы которого изложены в [29], использовано для верификации протокола Kerberos [9]. В общем виде данный подход представлен в [6].

Во всех приведенных выше работах предлагается использование некоторого конкретного способа верификации. В данной работе обосновывается необходимость комплексной методологии верификации

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

протоколов, использующей сильные стороны разных подходов, и в применении такой методологии для верификации конкретного протокола безопасности. Некоторые из описанных выше методов верификации предлагается использовать в качестве элементов предлагаемого подхода, поэтому они более подробно рассмотрены ниже.

3. Критерии выбора средств верификации. Как видно из приведенного обзора, разнообразие средств верификации, достаточно велико, что делает актуальной задачу формулировки четких критериев для сравнения средств верификации с целью выбора наиболее подходящего для решения конкретной задачи разработки протокола безопасности.

Предлагается выделить следующие свойства средств верификации:

— уровень автоматизации (чем больше степень автоматизации, тем лучше);

— простоту модели (ошибки возможны не только в протоколе, но и в его формальной модели, и вероятность таких ошибок возрастает с усложнением модели);

— гибкость в смысле выразительных свойств модели (чем меньше ограничений на моделируемые свойства, тем лучше);

— ограничения на модель в теоретико-вычислительном смысле (чем более сложные конфигурации можно промоделировать, тем лучше);

— ложные срабатывания при определении уязвимостей протокола (лучший вариант — без ложных срабатываний, приемлемый вариант — с небольшой вероятностью ложного обнаружения возможной атаки);

— извлечение алгоритма атаки (с точки зрения проектирования протокола возможность узнать способ использования уязвимости протокола предпочтительнее по сравнению с индикацией наличия уязвимости);

— наличие сообщества исследователей и/или разработчиков, использующих данное средство верификации (его наличие косвенным образом свидетельствует о достаточной выразительности средства и привлекательности для решения реальных задач).

Анализ имеющихся средств верификации показывает, что идеального (или близкого к идеальному) средства верификации, способного решить все проблемы оптимальным образом, не существует. Это означает, что для всесторонней верификации протокола безопасности требуется комбинация нескольких средств, позволяющая компенсировать

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

недостатки одного средства верификации за счет достоинств другого.

Данный подход требует анализа и классификации свойств существующих средств верификации (а также подходов, лежащих в их основе).

4. Анализ основных методов и средств верификации протоколов безопасности. Можно выделить два основных подхода к решению задачи верификации протоколов безопасности (и соответственно два класса методов верификации):

1) проверка на модели,

2) логический вывод (на основе доказательства свойств).

Некоторые средства верификации реализуют один из этих подходов в чистом виде, другие могут быть интерпретированы как реализация одного из этих подходов или же представляют ту или иную их комбинацию.

Представим далее оба этих подхода с рассмотрением реализующих их средств. Подробно анализируются наиболее характерные представители упомянутых подходов. Остальные средства рассматриваются более кратко, с указанием основных аспектов, которые отличают их от средств, рассматриваемых более подробно.

4.1. Проверка на модели. Класс методов верификации, основанных на проверке на модели, использует представление системы в виде набора состояний. При этом из множества состояний выделяется подмножество тех состояний, в которых нарушается тот или иной критерий безопасности. Верификация в данном случае сводится к доказательству того, что такое множество в данной модели пусто, либо система никогда не попадает ни в одно из них.

Для верификации могут использоваться средства проверки на модели общего назначения или средства, специально ориентированные на верификацию протоколов безопасности. За счет потери гибкости они позволяют упростить верификацию и (или) доказывать более сложные свойства.

4.1.1. Универсальные средства проверки на модели. К данной категории средств относятся SPIN, Murphi, а также FDR2 и PRISM.

Для верификации протоколов безопасности с использованием SPIN и Murphi необходимо:

— представить поведение участников протокола в виде, внешне напоминающем фрагмент программы на языке C (со специальными конструкциями, задающими обмен данными между участниками);

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

— аналогичным образом специфицировать поведение злоумышленника (в том числе перехват сообщений и генерацию новых сообщений на основе того, что уже известно злоумышленнику);

— описать критерии безопасности с использованием темпоральной логики (в терминах переменных, представляющих состояние/знание участников протокола и/или злоумышленника).

В силу того, что в Murphi и SPIN не представлена специфика верификации протоколов безопасности, описания получаются громоздкими.

FDR2 основан на использовании нотации CSP [16] для описания поведения участников протокола.

В отличие от Murphi и SPIN, FDR2 использует подход, который называется уточняющей проверкой на модели (*refinement model checking*). Он состоит в подтверждении того, что модель, описывающая поведение системы, реализующей проверяемый протокол, эквивалентна модели, задающей требования к данному протоколу (в данном случае речь идет о требованиях безопасности).

CSP является формализмом, оперирующим взаимодействующими процессами и операциями. Этим фактом определяется семантический разрыв между терминами, в которых специфицируются модели (процессы и взаимодействия между ними с помощью элементарных средств), и терминами предметной области (сообщения, шифрование, дешифрование, аутентификация и т. п.), что в конечном счете приводит к усложнению спецификации и понимания модели.

PRISM во многом похож на SPIN и Murphi. Его отличием является моделирование в вероятностных терминах. Это достигается путем расширения выразительных возможностей модели на основе возможности задавать несколько вариантов переходов из одного состояния в другие с назначением вероятности для каждого из вариантов.

4.1.2. Средства проверки на модели, ориентированные на верификацию протоколов безопасности. К данной категории средств относятся Casper, а также частично AVISPA.

Casper представляет собой надстройку над FDR2. Он позволяет описывать протоколы в подходящих терминах, а предоставляемый в рамках данного средства конвертор преобразует такое описание в CSP-модель. Это дает возможность использовать FDR2 для верификации моделей, описанных в терминах CSP.

Общая структура AVISPA представлена при описании базовых работ в области верификации протоколов безопасности. Три из входящих в состав AVISPA компонента могут быть отнесены к категории

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

средств проверки на модели. Это OFMC, SATMC и TA4SP.

Исходное описание протокола на универсальном языке HLPSL одинаково для всех компонентов AVISPA и дается в терминах, отражающих предметную область.

Говоря о верификаторах, входящих в состав AVISPA и упомянутых в данном разделе, заметим следующее. Общим моментом является то, что выполнение протокола безопасности представляется в рамках этих средств как работа машины состояний, и цели протокола интерпретируются в соответствии с критериями, определяющими подмножество множества состояний, в которые система не должна попадать.

Однако в отличие от универсальных средств типа SPIN и Murphi, в данном случае существуют способы, позволяющие существенно уменьшить зону исследования состояния системы, что позволяет значительно расширить границы применения данных средств.

После преобразования исходного описания протокола в промежуточное представление применяется одно из четырех средств верификации, каждое из которых основано на одном из следующих принципов:

— отложенные вычисления,

— логика ограничений,

— разрешение пропозициональной логической формулы,

— перезапись термов с аппроксимацией на бесконечное количество переходов.

Недостатки одного подхода могут компенсироваться достоинствами другого. Например решение с помощью перезаписи термов может не иметь сходимости (в отличие от отложенных вычислений и логики ограничений), однако в случае сходимости оно дает ответ для случая бесконечного количества сеансов протокола. В этом смысле данный подход достаточно гибок. В то же время он ограничен в плане набора проверяемых свойств, который определяется реализацией средства и в данный момент ограничен аутентификацией и конфиденциальностью.

4.2. Логический вывод. Класс методов верификации, основанных на логическом выводе, предполагает описание протокола и действий злоумышленника в рамках некоторой формальной логики. Критерий безопасности протокола в таком случае формулируется в виде утверждения в рамках данной формальной логики, после чего он должен быть доказан — возможно, с использованием автоматических или автоматизированных средств.

Как и в случае проверки на модели, существуют средства автоматизации доказательств общего назначения, а также средства, специ-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ально ориентированные на работу с протоколами безопасности.

4.2.1. Универсальные средства логического вывода. Характерным представителем данной группы средств верификации является Isabelle. Это средство для автоматизированного логического вывода, основанное на логике предикатов первого порядка.

Isabelle стоит особняком по отношению к другим средствам, рассматриваемым в настоящей работе, поскольку в нем используется принципиально иная парадигма взаимодействия средства верификации и разработчика протокола.

При использовании традиционных средств верификации разработчик формально описывает протокол, подает его спецификацию на вход средства верификации и получает ответ. При всех нюансах, свойственных каждому отдельному средству и разработчику (удобство языка описания, проблема эквивалентности реального протокола и его формального описания, возможность ложных срабатываний, необходимость интерпретации ответа от средства верификации и т. п.), общая последовательность действий остается той же.

При использовании Isabelle разработчик протокола должен построить логическую теорию и доказать в ее рамках различные утверждения. В силу теоретических ограничений данного подхода автоматическое доказательство невозможно. Однако отдельные фрагменты логического вывода можно выполнить автоматически. Основная трудность состоит в том, что пока определенное утверждение не доказано, нельзя сказать определенно, почему оно не доказано: потому, что оно невыводимо (и можно вывести его отрицание); или же потому, что еще не найден подходящий вывод. Это означает, что эффективность работы с Isabelle во многом зависит от начальных предположений, которые разработчик протокола делает на основании опыта и интуиции.

Все эти сложности компенсируются гибкостью, предоставляемой данным подходом, в рамках которого можно доказывать все то, что в принципе можно адекватно представить в рамках логики предикатов первого порядка.

4.2.2. Средства, ориентированные на верификацию протоколов безопасности. К данной категории средств можно отнести CAPLS, один из верификаторов, входящих в состав AVISPA (CL-AtSE), а также средство ProVerif.

Все они, используя разные подходы к верификации, позволяют задавать модель протокола в терминах, близких к моделируемой предметной области и в отличие от Isabelle позволяют в большинстве случаев получить тот или иной ответ о свойствах протокола. Лишь в не-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

которых случаях ProVerif может дать ложный ответ о наличии атаки. Другим ограничением ProVerif является невозможность определения алгоритма атаки — сообщается только лишь о ее возможности без позволения построить сценарий.

4.2.3. Средства, реализующие подход, основанный на уточнении шаблонов. В соответствии с подходом, реализованным в Scyther [12], протокол определяется как последовательность событий, причем к событиям относятся как передача сообщений, которыми обмениваются участники сеанса, так и сообщений, которые может вставлять злоумышленник. Используется нотация, позволяющая различать "нити" (отдельные исполнения того или иного события).

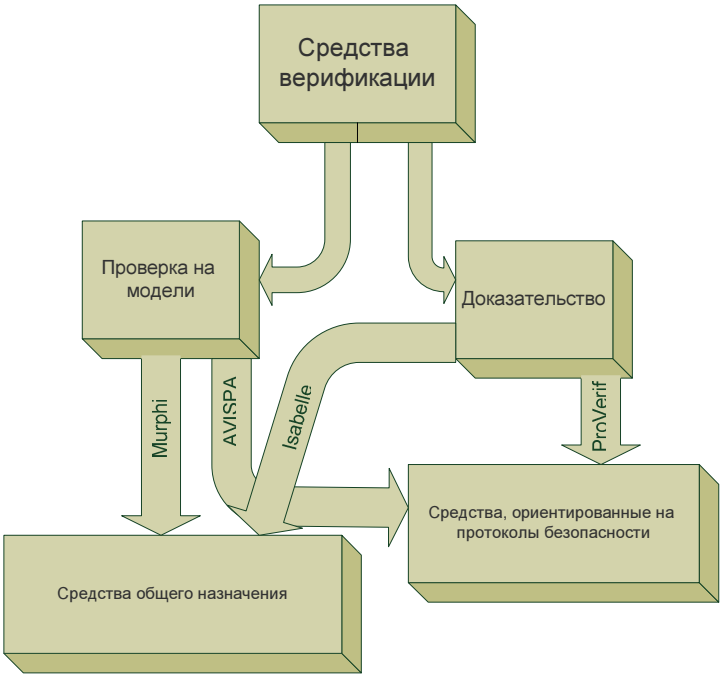
На множестве событий вводится специальное отношение, отражающее последовательность событий и являющееся частичным порядком. Получившийся в итоге направленный ациклический граф при определенных условиях понимается как шаблон протокола. С помощью такого шаблона можно представлять бесконечные трассы сообщений.

В результате применения алгоритма, подробно представленного в работе [12], либо доказывается, что протокол корректен для случая бесконечной трассы, либо доказывается, что он некорректен, либо предлагается доказательство корректности для ограниченного случая.

Кроме того, Scyther позволяет вводить в модель агента, подвергшегося атаке.

5. Комбинированные подходы к верификации. С точки зрения подходов к верификации основные рассмотренные средства верификации могут быть классифицированы так, как это показано на рисунке.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru



Средства верификации протоколов безопасности.

Средство AVISPA, предоставляющее удобные средства спецификации моделируемого протокола, ограничено в плане проверяемых свойств. Будучи комбинированным с точки зрения использования различных подходов к доказательству заданных свойств, оно жестко ограничивает набор свойств, подлежащих проверке (на уровне языка HLPSL). Кроме того, не удалось обнаружить ни одной реально существующей сторонней реализации модуля доказательства свойств, что затрудняет вывод о работоспособности и условиях применения такого механизма. В итоге AVISPA, удовлетворяя требованиям по большинству параметров, не является гибким с точки зрения набора моделируемых свойств.

В то же время универсальное с точки зрения проверяемых свойств средство Isabelle не позволяет описывать проверяемый протокол удобным образом, а также требует для работы специфических навыков.

Отсутствие единственного идеального средства обусловливает

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

необходимость комбинирования нескольких средств для решения задачи верификации.

Выделим два варианта комбинирования средств верификации:

1) использование разных средств для проверки разных свойств,

2) обобщение с помощью Isabelle.

В рамках первого подхода предполагается, что средства, ориентированные на верификацию протоколов безопасности (например, AVISPA, ProVerif), используются для верификации стандартных свойств (конфиденциальности, аутентификации), в то время как универсальные средства применяются для верификации более сложных свойств.

В соответствии со вторым подходом возможности Isabelle используются для обобщения частных свойств, проверенных с помощью других средств. Необходимость такого подхода можно кратко обосновать следующим образом. В целях упрощения верификации обычной практикой является формальное описание упрощенного и ограниченного случая, после чего неформальным образом полученный результат интерпретируется как покрывающий поведение протокола в общем случае. Для более строгого обобщения можно использовать универсальное средство Isabelle, которое позволяет получить строгое доказательство корректности обобщения вместо неформальной интерпретации.

В работе авторов по проектированию и верификации EnTrusting-протокола ([1–3]) применяются средства AVISPA и Isabelle.

Совместное применение этих средств в настоящее время основано на варианте комбинирования “разные средства для разных свойств”. Для проверки классических и хорошо изученных свойств, например конфиденциальности и аутентификации в случае атаки “man-in-the-middle” (“человек посередине”), используется более удобное и хорошо приспособленное для этого средство AVISPA. Для верификации менее традиционных и изученных свойств, таких как конфиденциальность и аутентификация в случае атаки “man-in-the-end” (“человек на конце”), а также свойств, связанных с особенностями реализации модулей и тегов или с временными характеристиками протокола, используется средство Isabelle [2].

На данный момент с помощью AVISPA разработаны модели для проверки аутентификации в случае атаки “man-in-the-middle”. Модели с использованием Isabelle для случаев, описанных выше, в данный момент находятся в стадии разработки. В то же время в целях исследования возможностей Isabelle это средство использовано для доказательства классических свойств.

Сводная оценка средств верификации представлены в таблице.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Сводная оценка средств верификации

Критерий	Murphi/SPIN	AVISPA	Isabelle	ProVerif	Scyther
Уровень автоматизации	Автоматическая верификация	Автоматическая верификация	Автоматизированная верификация, под «ручным» управлением	Автоматическая	Автоматическая
Простота модели	Модель — сложная, модель злоумышленника описывается явным образом	Модель — несложная, модель злоумышленника является встроенной	Модель — сложная, модель злоумышленника задается как часть общей модели	Модель — несложная	Модель — несложная
Гибкость подхода	Высокая	С точки зрения подходов к моделированию — высокая, с точки зрения моделируемых свойств — низкая	Высокая	Нет	Нет
Ложные срабатывания	Без оптимизации — нет, с оптимизацией — возможны	Нет	Возможна неопределенность в ходе доказательства	Возможны	Нет
Ограничения	Существенные, определяются полным перебором, лежащим в основе подхода (что вызывает комбинаторный взрыв)	Зависит от применяемого подхода	Теоретические ограничения логики предикатов первого порядка	Фиксированный набор свойств, подлежащих верификации	Фиксированный набор свойств, подлежащих верификации
Извлечение алгоритма атаки	Есть возможность	Есть возможность	Не гарантировано	Не гарантировано	Есть
Сообщество разработчиков	Murphi — нет, SPIN — нет	Есть	Есть	Нет	Нет

Из таблицы видно, что ни одно из средств верификации протоколов безопасности не обладает идеальным набором свойств. Это значит, что ни одному из них нельзя отдать предпочтение как “лучшему” средству верификации.

Как известно, полная верификация протокола с описанием всех деталей приводит к чрезмерно громоздкой модели. Поэтому обычно моделируется только часть протокола — возможно, с некоторыми до-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

пущениями, которые должны быть учтены при интерпретации результатов протокола.

В частности, при проверке конфиденциальности на этапе инициализации сеанса первоначально было сделано предположение о том, что аутентичность сервера по отношению к клиенту не гарантирована. Это не противоречит предположению о доверенном сервере — клиент, общающийся с сущностью, выдающей себя за доверенный сервер, может быть не уверен в том, что его партнер является таковым.

Рассмотрим наиболее важные фрагменты разработанной модели [2].

Первый шаг сервера описывается, как это показано на листинге 1.

```
role server (S, C: agent, K : symmetric_key, SND, RCV: channel (dy))
…
transition
// Получив в начальном состоянии системное сообщение start
// (индикатор начала сеанса)
        0.  State  = 0 /\ RCV(start) =|>
// Сервер переходит в следующее состояние
// и посылает клиенту зашифрованный модуль.
                State':= 2 /\  SND({Module0}_K)
…
end role
```

Листинг 1. Поведение сервера.

Первый шаг клиента выглядит, как показано на листинге 2.

```
role client(S, C: agent, K : symmetric_key, SND, RCV: channel (dy))
…
transition
// Получив в состоянии 1 зашифрованный модуль
        1.  State  = 1  /\ RCV({Module0}_K) =|>
// клиент переходит в состояние 3 и посылает серверу зашифрованный тег
                State':=3 /\ SND({Tag0}_K) /\
                secret(Tag0, p, {S,C})
…
end role
```

Листинг 2. Поведение клиента.

Следует обратить внимание на предикат secret (Tag0, p, {S,C}). Он не связан с действиями участников сеанса, а описывает критерий конфиденциальности — данные Tag0 могут быть известны только участникам S и C, а p привязывает данный предикат к разделу модели, описывающему проверяемые цели:

Роль environment, описывающая моделируемую систему в целом, выглядит, как показано на листинге 3:

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

```
role environment() def=…
// начальное знание злоумышленника(идентификаторы клиента и сервера,
// а также симметричные ключи сервер-злоумышленник и
// клиент-злоумышленник)
intruder_knowledge={s,c,ksi,kic}…
composition
// параллельная работа трех сеансов: сервер-клиент, сервер-злоумышленник
// и злоумышленник-клиент
session(s,c,ksc)/\session(s,i,ksi)/\session(i,c,kic)
…
end role
```

Листинг 3. Поведение клиента

Запуск AVISPA с верификатором CL-AtSe дает следующий результат, показанный на листинге 4.

```
SUMMARY
UNSAFE
…
ATTACK TRACE
i -> (s,6):  start
(s,6) -> i:  {dummy_msg}_ksi
i -> (s,3):  start
(s,3) -> i:  {dummy_msg}_ksc
i -> (c,10):  {dummy_msg}_kic
(c,10) -> i:  {dummy_nonce}_kic
        & Secret(dummy_nonce,set_65);
        Add i to set_65;
        Add c to set_65;
i -> (c,4):  {dummy_msg}_ksc
(c,4) -> i:  {dummy_nonce}_ksc
        & Secret(dummy_nonce,set_59);
        Add s to set_59;
        Add c to set_59;
```

Листинг 4. Результат работы верификатора

Данный результат работы верификатора можно интерпретировать следующим образом (листинг 5):

```
// (1) сначала злоумышленник соединяется с сервером как клиент
i->(s,6):start
(s,6)->i:{dummy_msg}_ksi

// (2) затем злоумышленник убеждает добросовестного клиента начать
//сеанс с сервером
i->(s,3):start
(s,3)->i:{dummy_msg}_ksc

// (3) наконец злоумышленник подменяет сервер для добросовестного
// клиента, посылает ему модуль и получает тег
i -> (c,10):  {dummy_msg}_kic
```


Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

```
(c,10) -> i:  {dummy_nonce}_kic
     & Secret(dummy_nonce,set_65);
     Add i to set_65;
     Add c to set_65;
```

Листинг 5. Интерпретация результата работы верификатора

Интерпретируя результат верификации, следует отметить, что мы сделали предположение о не гарантированности аутентификации сервера для клиента.

Этому предположению соответствует сеанс “session(i,c,kic)” в описании роли environment. После удаления этого предиката из модели верификатор сообщает о безопасности протокола.

Заключение. В условиях возрастающей сложности конфигурации сетей и возрастания степени их открытости, вызванной экономической необходимостью, крайне важным является обеспечение надежности обмена данными и противодействия действиям возможных злоумышленников.

Для решения данных проблем применяются протоколы безопасности, при разработке которых, однако, не исключены технические решения, оставляющие злоумышленникам возможности для атак.

Разработанные к настоящему моменту средства верификации протоколов безопасности частично решают эту задачу.

Однако, как можно видеть из настоящего обзора, они предлагают решение лишь частных задач, а данные, полученные в результате верификации, требуют нетривиальной интерпретации.

Вопрос универсального подхода к исчерпывающему решению общей проблемы надежности протоколов безопасности по-прежнему остается открытым.

Более того, есть все основания полагать, что в силу существующих объективных ограничений теоретического характера найти такое универсальное решение невозможно.

В этих условиях представляется целесообразным применение комбинации различных средств верификации. При этом реально достижимой целью представляется переход от комбинации средств, исходя из общих соображений (как это фактически делается в настоящее время), к их комбинации на основе строгой методологии.

Настоящая работа является шагом в данном направлении, предоставляя классификацию существующих средств верификации и предлагая несколько схем комбинирования различных средств.

Предложенные схемы комбинирования средств верификации призваны решить проблему неполноты существующих подходов в двух

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

измерениях:

1) с точки зрения набора проверяемых свойств,

2) с точки зрения адекватности модели проверяемому протоколу.

С точки зрения набора проверяемых свойств, комбинирование основано на построение нескольких моделей разными средствами. Для развития данной идеи требуется более детальная классификации средств верификации, позволяющая принять оптимальное решение о наборе средств, необходимых и достаточных для решения поставленной задачи.

С точки зрения адекватности модели проверяемому протоколу, комбинирование построено на применении средств автоматизированного доказательства теорем для проверки утверждений о том, что модель, проверяющая свойства для части проверяемого протокола, адекватна потенциальной модели полного протокола с точки зрения проверяемых свойств.

Развитие предложенных идей дает возможность разработки целостной и строгой методологии комбинирования различных средств верификации для комплексного решения проблемы доказательства корректности протоколов безопасности.

Основными направлениями будущей работы являются дальнейшее исследование предложенных комбинированных подходов, а также создание новых вариантов комбинирования.

Литература

1. *Десницкий В. А., Котенко И. В.* Защита программного обеспечения на основе механизма “удаленного доверия” // Изв. вузов. Приборостроение, Т. 51, № 11. 2008, С. 26–30.
2. *Десницкий В. А., Котенко И. В., Резник С. А.* Разработка и верификация протокола обмена сообщениями для защиты программ на основе механизма “удаленного доверия” // Защита информации. Инсайд. 2008. № 4. С. 59–63; № 5, 2008. С. 68–74.
3. *Котенко И. В., Десницкий В. А.* Аспектно-ориентированный подход к реализации мобильного модуля в модели защиты, основанной на механизме “удаленного доверия” // Информационные технологии и вычислительные системы. 2008. № 5.
4. *Косачев А. С., Пономаренко В. Н.* Анализ подходов к верификации функций безопасности и мобильности. М.: Триумф, 2004. 101 с.
5. *Abadi M., Blanchet B., Fournet C.* Just Fast Keying in the Pi Calculus // ACM Transactions on Information and System Security. TISSEC. July 2007. Vol. 10, № 3. P. 1–59.
6. *Bella G.* Inductive Verification of Cryptographic Protocols. PhD Thesis, University of Cambridge, 2000. 189 p.
7. *Blanchet B.* An Efficient Cryptographic Protocol Verifier Based on Prolog Rules // Proc. of 14th IEEE Computer Security Foundations Workshop (CSFW–14). Cape Breton, Nova Scotia, Canada, IEEE Computer Society, June 2001. P. 82–96.
8. *Basin D., Mödersheim S., Viganò L.* An On-The-Fly Model-Checker for Security Protocol Analysis // Proc. of ESORICS'03, Lecture Notes in Computer Science. 2003. Vol.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

2808. P. 253–270.
9. *Bella G., Paulson L. C.* Using Isabelle to Prove Properties of the Kerberos Authentication System // Proc. of DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997. 11 p.
10. *Clark J., Jacob J.* A Survey of Authentication Protocol Literature: Version 1. 0. http://www. cs. york. ac. uk/jac/papers/ drareview. ps. gz, 1997. 109 p.
11. *Compagna L.* SAT-based Model-Checking of Security Protocols. PhD Thesis, Universita degli Studi di Genova and the University of Edinburgh, September 2005. 216 p.
12. *Cremers C. J. F.* Unbounded Verification, Falsification, and Characterization of Security Protocols by Pattern Refinement // Proc. of the 15th ACM conference on Computer and communications security, 2008. P. 119–128.
13. *Durgin N., Lincoln P., Mitchell J., Scedrov A.* Undecidability of bounced security protocols // Proc. of the FLOC'99 Workshop on Formal Methods and Security Protocols (FMSP'99), 1999.
14. *Denker G., Millen J.* CAPSL integrated protocol environment // Proc. of DARPA Information Survivability Conference, DISCEX 2000. IEEE Computer Society, 2000. P. 207–221.
15. *Gritzalis S., Spinellis D., Georgiadis P.* Security protocols over open networks and distributed systems: Formal methods for their analysis, design, and verification // Computer Communications. May 1999. Vol. 22, № 8. P. 695–707.
16. *Hoare C. A. R.* Communicating sequential processes // Communications of the ACM, 1978. Vol. 21, № 8. P. 666–677.
17. *Josang A.* Security Protocol Verification Using SPIN // Proc. of SPIN'95 Workshop, 1995. 9 p.
18. *Lowe G.* An attack on the Needham-Schroeder public key authentication protocol // Information Processing Letters, November 1995. Vol. 56, № 3. P. 131–136.
19. *Lowe G.* Breaking and Fixing the Needham-Schroeder Public-Key Protocol Using FDR Tools and Algorithms for Construction and Analysis of Systems // Proc. of the Second International Workshop, TACAS 96, Passau, Germany, March 27–29, 1996. Lecture Notes in Computer Science. 1996. Vol. 1055. P. 147–166.
20. *Lowe G.* Casper: A Compiler for the Analysis of Security Protocols // J. of Computer Security. 1998. Vol. 6, № 1–2. P. 53–84.
21. *Meadows C.* Formal Verification of Cryptographic Protocols: A Survey // Proc. of ASIACRYPT. 1994. P. 135–150.
22. *Meadows C.* Formal methods for cryptographic protocol analysis: emerging issues and trends // IEEE J. on Selected Areas in Communications. January 2003. Vol. 21, Issue 1. P. 44–54.
23. *Mitchell J. C., Mitchell M., Stern U.* Automated analysis of cryptographic protocols using Murphi // IEEE Symposium on Security and Privacy, 1997. P. 141–151.
24. *Millen J., Shmatikov V.* Constraint Solving for Bounded-Process Cryptographic Protocol Analysis // Proc. of the ACM Conference on Computer and Communications Security, 2001. P. 166–175.
25. *Mitchell J. C., Shmatikov V., Stern U.* Finite-State Analysis of SSL 3. 0 // 7th USENIX Security Symposium, 1998. 15 p.
26. *Nieh B. and Tavares S.* Modeling and analyzing cryptographic protocols using Petri nets. // Proc. of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, 1992. Vol. 718. P. 275–295.
27. *Norman G., Shmatikov V.* Analysis of Probabilistic Contract Signing // J. of Computer Security, 2006, Volume 14 , Issue 6. P. 561–589.
28. *Oehl F., Cece G., Kouchnarenko O., Sinclair D.* Automatic Approximation for the

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Verication of Cryptographic Protocols // Proc. of the International Conference on Formal Aspects of Security (FASec), London, UK. Lecture Notes in Computer Science. November 2003. Vol. 2629. P. 33–48.
29. *Paulson L. C.* The foundation of a generic theorem prover // J. of Automated Reasoning, September 1989. Vol. 5, Issue 3. P. 363–397.
30. *Rusinowitch M.* Automated Analysis of Security Protocols // Proc. of the 12th Intern. Workshop on Functional and (Constraint) Logic Programming (WFLP'03). Electronic Notes in Theoretical Computer Science. 2003. Vol. 86, № 3. 4 p.
31. *Shmatikov V.* Probabilistic Model Checking of an Anonymity System // J. of Computer Security, 2004. Vol. 12, № 3. P. 355–377.
32. *Viganò L.* Automated Security Protocol Analysis with the AVISPA Tool // Proc. of the XXI Mathematical Foundations of Programming Semantics (MFPS'05), ENTCS, Elsevier, 2005. № 155. P. 61–86.

Котенко Игорь Витальевич — д-р техн. наук, проф.; руководитель научно-исследовательской группы компьютерной безопасности Санкт-Петербургского Института Информатики и автоматизации РАН (СПИИРАН). Область научных интересов: Безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер-терроризму, искусственный интеллект, в том числе многоагентные системы, мягкие и эволюционные вычисления, машинное обучение, извлечение знаний, анализ и объединение данных, интеллектуальные системы поддержки принятия решений, телекоммуникационные системы, в том числе поддержка принятия решений и планирование для систем связи. Число научных публикаций — более 450. Адрес: ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; раб. тел. +7(812)328-2642, факс +7(812)328-4450.

Резник Сергей Александрович — соискатель научно-исследовательской группы компьютерной безопасности Санкт-Петербургского Института Информатики и автоматизации РАН (СПИИРАН). Область научных интересов: верификация протоколов безопасности. Число научных публикаций — 9. sergey.reznick@sun.com, www.comsec.spb.ru; «Сан Майкросистемс», ул. 10-я Красноармейская, 22А, Санкт-Петербург, 190103, РФ; р.т. +7(812)334-6101, факс +7(812)334-6238. Научный руководитель — И.В. Котенко.

Шоров Андрей Владимирович — аспирант научно-исследовательской группы компьютерной безопасности Санкт-Петербургского Института Информатики и автоматизации РАН (СПИИРАН). Область научных интересов: Защита компьютерных сетей от инфраструктурных атак. Число научных публикаций — 5. Адрес: ashorov@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В. О., д. 39, Санкт-Петербург, 199178, РФ; раб. тел. +7(812)328-2642, факс +7(812)328-4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект №07–01–00547), программы фундаментальных исследований ОНИТ РАН и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза RE-TRUST (контракт № 021186–2).

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru