ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

СОВЕТ МОЛОДЫХ УЧЕНЫХ

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2014» атты IX халықаралық ғылыми конференциясы

IX Международная научная конференция студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2014»

The IX International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION-2014»

2014 жыл 11 сәуір
11 апреля 2014 года
April 11, 2014

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2014» атты IX Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ IX Международной научной конференции студентов и молодых ученых «Наука и образование - 2014»

PROCEEDINGS of the IX International Scientific Conference for students and young scholars «Science and education - 2014»

2014 жыл 11 сәуір

Астана

УДК 001(063)
ББК 72
Ғ 96

Ғ 96

«Ғылым және білім – 2014» атты студенттер мен жас ғалымдардың IX Халықаралық ғылыми конференциясы = IX Международная научная конференция студентов и молодых ученых «Наука и образование - 2014» = The IX International Scientific Conference for students and young scholars «Science and education - 2014». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2014. – 5831 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-610-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(063)
ББК 72

ISBN 978-9965-31-610-4

сознательным игроком, хотя и не противодействующим Первой компании, но преследующим свою собственную цель. А именно, она ищет стратегию гарантированно минимальных выплат против компании, составляющей портфель максимально гарантированной эффективности.

С этой точки зрения Первый игрок – это инвестор, он решает, в каких долях вкладывать, причем работает в условиях неопределенности и пытается составить портфель максимально гарантированной эффективности. Первый игрок выбирает доли, обладающие свойствами вероятностей, то есть выбирает смешанную стратегию в матричной игре. Второй игрок – это «природа». В нашем случае эта Вторая компания не противодействует Первой, а преследует собственные цели минимизации дивидендных выплат. Вторая компания («природа») выбирает смешанную стратегию (y_j). В этой матричной игре нужно найти равновесие. Оно существует, как в любой матричной игре. Для инвестора – это выбор портфеля максимально гарантированной эффективности (как определено выше), а для «природы» - вероятности появления вариантов $\overline{j=1,m}$.

Список использованных источников

1. Нуртазина К.Б. Оптимизация портфеля ценных бумаг и управление в условиях неопределенности: Монография – М.: ГУУ, 2011.

УДК 004.4

АВТОМАТИЧЕСКАЯ ВЕРИФИКАЦИЯ ПРОТОКОЛОВ

Мұса Асхар Шүкірұлы
askhar@inbox.ru
магистрант специальности «6М070500 Математическое и компьютерное моделирование»
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – М.Бекенов

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 преобразований,

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

В данное время опубликовано несколько работ, посвященных анализу подходов к верификации протоколов безопасности.

В 2005 г. появился новый программный продукт — AVISPA (Automated Validation of Internet Security Protocols and Applications) [1], разработанный в рамках международного проекта, в котором участвовали LORIA —INRIA (Франция), ETH (Цюрих, Швейцария), Университет Генуи (Италия), Siemens AG (Германия). Судя по заявлениям его разработчиков, продукт AVISPA должен стать прорывом в области анализа криптопротоколов. Разработка данного средства рассматривается как единый европейский проект, реализуемый с участием многих ведущих институтов и организаций европейских стран. Он интегрирует различные современные подходы к анализу протоколов, такие как проверка на модели (model-checking), древовидные автоматы, временная логика. При этом используются разработки, созданные после 2000 г. Специально для него были разработаны версии языков HLPSL (High-Level Protocols Specification Language) [2] и IF (Intermediate Format) [3], позволившие существенно расширить класс изучаемых протоколов, а также интегрировать в единую платформу сразу несколько различных методов.

В отличие от других средств исполняемый программный код этого средства доступен через Интернет. Поэтому изучение этого средства представляет большой интерес как с точки

зрения исследования возможностей реализованного в нем подхода, так и с точки зрения применения его на практике. Польная информация о разработке продукта AVISPA и публикациях, лежащих в его основе, доступна на интернет-сайте http://www.avispa-project.org.

Структура средства AVISPA показана на рисунке 1.

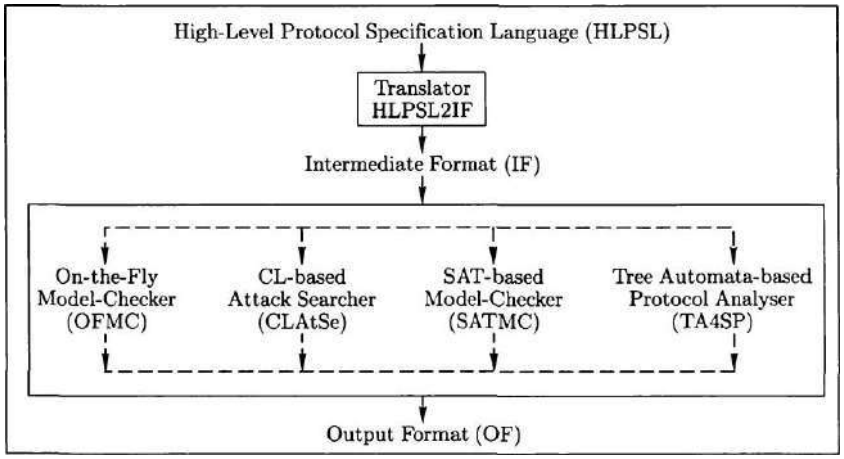

Рисунок 1 – Структура средства AVISPA

Принцип его работы состоит в следующем: сначала составляют спецификацию исследуемого протокола на языке HLPSL и записывают в файл с расширением *.hlpsl. Это язык высокого уровня, основанная на ролях: независимые базовые роли для каждого участника и композиционные роли для представления сценариев базовых ролей.

Спецификация на языке HLPSL транслируется в промежуточный формат IF с использованием транслятора HLPSL2IF. Промежуточный формат IF представляет собой язык более низкого уровня, чем язык HLPSL, который компилируется непосредственно выходными модулями средства AVISPA. Это преобразование прозрачно для пользователя, так как транслятор работает автоматически. Более подробно о промежуточном формате можно прочитать в публикациях [3, 4].

После поступления на вход средства AVISPA спецификации протокола на языке IF он проверяется на предмет выполнения или нарушения указанных целей безопасности. В настоящее время средство AVISPA включает четыре выходных модуля:

1) OFMC (On-the-Fly Model-Checker);
2) CLAtSe (CL-based Attack Searcher);
3) SATMC (SAT-based Model-Checker);
4) TA4SP (Tree Automata-based Protocol Analyser).

Этот список может быть в дальнейшем расширен. Данные модули частично дублируют и взаимно дополняют друг друга.

Работа [5] 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 [6] описывается метод верификации, используемый компоненте CLAtSe (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 [7]. 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 [8] 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 настоящее время осуществляется доработка и тестирование средства AVISPA. В качестве основы для тестирования выбрана библиотека протоколов, встречающихся в документах IETF. Результаты и проблемные ситуации, возникающие при анализе протоколов, отражаются в документах [9, 10].

Другие средства. Помимо AVISPA в первое десятилетие XXI в. появились и другие автоматизированные инструментальные средства анализа протоколов, реализованные в рамках различных национальных проектов. Здесь следует упомянуть такие средства, как Proverif (INRIA, Франция), HERMES (проект EVA, Франция), Scyther (ETH, Цюрих) и др. Они представляют собой мощные интегрированные, основанныена последних достижениях верификационной техники и автоматического доказательства средства анализа протоколов, которые позволяют анализировать протокол как для конечного, так и для бесконечного числа сеансов.

Список использованных источников

1. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. The AVISPA Tool. – 2005. – http://www.avispa-project.org/publications.html.
2. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. Deliverable 2.1 The High-Level Protocol Specification Language. – 2003. – http://www.avispa-project.org/publications.html.
3. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. Deliverable 2.3 The Intermediate Format. – 2003. – http://www.avispa-project.org/publications.html.
4. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. The AVISPA v.1.1 User Manual. – 2006. – http://www.avispa-project.org/publications.html.
5. Basin D., Modersheim S., Vigano L. An On-The-Fly Model-Checker for Security Protocol Analysis // Proc. of ESORICS'03, Lecture Notes in Computer Science. 2003. Vol. 2808. P. 253–270.
6. 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.
7. 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.
8. Oehl F., Cece G., Kouchnarenko O., Sinclair D. Automatic Approximation for the 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.
9. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. Deliverable D6.1 List of Selected Problems. – 2005. – http://www.avispa-project.org/publications.html.
10. Automated Validation of Internet Secutiry Protocols and Applications (AVISTA). IST-2001-39252. Deliverable D6.2 Specification of the Problems in the High-Level Specification Language. – 2005. – http://www.avispa-project.org/publications.html.

УДК:303.725.23:631.145(045)