

ПРОГРАММИСТУ

П. Торстейнсон
Г. А. Ганеш

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ В ТЕХНОЛОГИИ .NET



Лаборатория
ЗНАНИЙ

**КРИПТОГРАФИЯ
И БЕЗОПАСНОСТЬ
В ТЕХНОЛОГИИ
.NET**

EXPERT PRACTITIONERS. SEASONED INSTRUCTORS
.NET

.NET SECURITY AND CRYPTOGRAPHY

PETER THORSTEINSON
G. GNANA ARUN GANESH



Prentice Hall PTR, Upper Saddle River, NJ 07458
www.phptr.com

ПРОГРАММИСТУ

П. Торстейнсон, Г. А. Ганеш

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ В ТЕХНОЛОГИИ .NET

Перевод с английского

В. Д. Хорева

под редакцией

С. М. Молявко

4-е издание, электронное



Москва
Лаборатория знаний
2020

УДК 004.7
ББК 32.973.202
Т61

Серия основана в 2005 г.

Торстейнсон П.

Т61 Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. — 4-е изд., электрон. — М. : Лаборатория знаний, 2020. — 482 с. — (Программисту). — Систем. требования: Adobe Reader XI ; экран 10". — Загл. с титул. экрана. — Текст : электронный.
ISBN 978-5-00101-700-4

Подробно излагаются вопросы реализации на .NET-платформе симметричной и асимметричной криптографии, цифровых подписей, XML-криптографии, пользовательской безопасности и защиты кодов, ASP .NET-безопасности, безопасности Web-служб. Изложение построено на разборе примеров конкретных атак на системы безопасности, содержит большое количество текстов отлаженных программ.

Для программистов, занимающихся разработкой и настройкой систем безопасности на платформе .NET.

**УДК 004.7
ББК 32.973.202**

Деривативное издание на основе печатного аналога: Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. — М. : БИНОМ. Лаборатория знаний, 2007. — 479 с. : ил. — (Программисту). — ISBN 978-5-94774-312-8.

Authorized Translation from the English language edition, entitled .NET SECURITY AND CRYPTOGRAPHY; by PETER THORSTEINSON; and by G. GANESH; published by Pearson Education, Inc, publishing as Prentice Hall. Copyright © 2004 by Pearson Education, Inc. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc. Electronic RUSSIAN language edition published by BKL PUBLISHERS. Copyright © 2013.

Авторизованный перевод издания на английском языке, озаглавленного .NET SECURITY AND CRYPTOGRAPHY, авторы PETER THORSTEINSON и G. GANESH, опубликованного Pearson Education, Inc, осуществляющим издательскую деятельность под торговой маркой Prentice Hall. Copyright © 2004 by Pearson Education, Inc. Все права защищены. Воспроизведение или распространение какой-либо части/частей данной книги в какой-либо форме, какими-либо способами, электронными или механическими, включая фотокопирование, запись и любые поисковые системы хранения информации, без разрешения Pearson Education, Inc запрещены. Электронная русскоязычная версия издана BKL Publishers. Copyright © 2013.

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации

© 2004, Pearson Education, Inc.,
Publishing as Prentice Hall
Professional Technical Reference.
Upper Saddle River, New Jersey 07458.
© русское издание, Лаборатория
знаний, 2015

ISBN 978-5-00101-700-4

Предисловие

За последние несколько лет криптография в частности и технологии обеспечения безопасности вообще непрерывно повышали свою значимость для пользователей Windows и производителей программного обеспечения. С другой стороны функции обеспечения безопасности (и криптографические функции в том числе) 32-разрядных систем семейства Windows стали сопоставимы с аналогичными функциями больших компьютерных платформ, где такие функции издавна имели высокий приоритет. Теперь же, с широким внедрением .NET, реализация функций обеспечения безопасности на персональных компьютерах стала делом более простым, чем когда-либо ранее. Разумеется, все еще требуются значительные усилия, для того чтобы понять и освоить базовые концепции, а также приобрести навыки, необходимые для обращения с соответствующими функциональными возможностями .NET. (Кстати, это как раз и есть тема данной книги.) И хотя многие из этих функций были доступны и раньше в скрытой форме библиотек Windows, именно появление платформы .NET делает программирование с использованием криптографии и других технологий обеспечения безопасности гораздо более простым, а его результаты – гораздо более мощными, чем когда-либо ранее. Платформа .NET Security Framework позволяет использовать широкий набор специальных классов, которые относительно нетрудно освоить, и все эти возможности мы исследуем в нашей книге.

Книга призвана исчерпывающе осветить все практические вопросы в реализации криптографических и иных, связанных с безопасностью, функциональных возможностей в приложениях .NET. Она представляет собой эффективное учебное пособие, содержащее множество ясных и наглядных примеров исходного кода.

Организация книги

Структура книги включает в себя десять глав и пять приложений. Глава 1 вводит читателя в тематику криптографии и безопасности на платформе .NET и содержит еще нетехнический обзор тех тем, которые гораздо детальней освещены в последующих главах. Также в этой первой главе приведены рассуждения о структуре книги и о том, как в ней соотносятся темы криптографических функций и других функций, связанных с безопасностью. Цель этой главы не состоит в том, чтобы достичь сколько-нибудь глубокого понимания или изучить примеры кода, но она должна привести читателя к концептуальному пониманию криптографических и

других, связанных с безопасностью, технологий, на платформе .NET. Глава 2 обеспечивает знакомство с теорией, достаточное для более глубокого понимания материала последующих глав. Главный ее посыл состоит в том, что все технологии безопасности основываются, в конечном счете, на криптографии, а для многостороннего понимания криптографии необходимо вначале освоить несколько базовых теоретических криптографических концепций. Главы 3, 4, 5 и 6 содержат детально проработанные примеры программирования в .NET, относящиеся к симметричным алгоритмам, асимметричным алгоритмам, цифровым подписям и XML-криптографии, соответственно. Главы 7 и 8 описывают программирование в .NET с использованием концепции идентификации пользователей и концепции прав доступа к коду, соответственно. Глава 9 введет вас в тему программирования на основе технологии ASP.NET, а глава 10 познакомит с программированием Web-служб на основе ASP.NET.

Все аспекты криптографии и безопасности в .NET рассматриваются в подходящем контексте и в должной последовательности в приложениях, где они в реальности чаще всего применяются. Приложения к книге описывают несколько дополнительных тем таких, как способы атаки на выполняющийся код и некоторые математические темы, связанные с криптографией.

Эта книга задумана, как практическое учебное пособие с множеством примеров программ, которые иллюстрируют конкретные вопросы и концепции. Мы здесь концентрируемся скорее на вопросах практического программирования задач безопасности в .NET, чем на системном администрировании. Эта книга обеспечивает достаточно общей информации, чтобы читатель понял, почему вопросы безопасности и криптография столь важны при разработке современного программного обеспечения. Цель книги состоит в том, чтобы научить читателя создавать серьезные приложения с использованием платформы .NET Security Framework. Эта книга является частью серии «The Integrated .NET Series» от Object Innovations и Prentice Hall PTR.

Примеры программ

Лучший способ изучить какую-то серьезную библиотеку классов (например, такую, как .NET Security Framework) состоит в том, чтобы изучить и написать на ней много программ. В этой книге содержится большое число небольших программ, которые иллюстрируют каждую из используемых на практике возможностей .NET Security Framework в отдельности, что облегчает их понимание. Программы (полностью или частично) приводятся в тексте книги (с переведенными комментариями и сообщениями), и все они имеются в программном приложении к книге (с оригинальными комментариями и сообщениями). Эти примеры программ представлены в виде самораспаковывающегося архивного файла на Web-сайте этой книги. После распаковки архива будет создана структура каталогов по пути (по умолчанию) C:\OI\NetSecurity. Все примеры про-

грамм (они начинают появляться в книге, начиная с главы 2) распределены по каталогам Chap02, Chap03 и так далее. Все примеры, относящиеся к одной главе, находятся в отдельных папках внутри каталога соответствующей главы. Имена папок ясно идентифицируют содержащиеся в них примеры программ.

Эта книга является частью серии «The Integrated .NET Series». Примеры программ для других книг этой серии находятся в своих каталогах внутри каталога \OI, поэтому все программы из всех книг серии будут находиться в одном месте. Эти программы предназначены только для целей обучения, и их нельзя использовать ни в каком программном продукте. Все программы, включая инструкции по их использованию, предоставляются на условиях «как есть», и любого рода претензии к ним не принимаются.

Web-сайт

Web-сайт для книг этой серии находится по адресу <http://www.objectinnovations.com/dotnet.htm>.

Ссылка на этот Web-сайт приведена для загрузки примеров программ для этой книги.

Благодарности

Питер Торстейнсон (Peter Thorsteinson)

Мы хотели бы поблагодарить Джилл Хэрри (Jill Harry) из Прентис Холл за ее поддержку в начинании этого проекта. Также мы благодарны редактору серии Роберту Обергу (Robert Oberg) за его ценную помощь.

Дж. Гнана Арун Ганеш (G. Gnana Arun Ganesh)

Я хотел бы поблагодарить моих родителей Дж. А. Гнанавел (G. A. Gnanaivel) и Дж. Н. Вадивамбал (G. N. Vadivambal) за их безграничную любовь, терпение, поддержку и воодушевление. Также я благодарю мою сестру Дж. Дж. Сарадха (G. G. Saradha) за ее любовь, нежность и товарищескую поддержку. Моя глубочайшая благодарность адресована моему доброму ангелу, д-ру Роберту Обергу (Robert Oberg), который воодушевлял меня на протяжении всего этого замечательного проекта. Также я благодарен мистеру Анидо Ди (Anido Dey), мистеру Нарайана Рао Сурапанени (Narayanan Rao Surapaneni) и мистеру Виноду Кумару (Vinod Kumar) за то, что они воодушевляли меня и побуждали двигаться вперед. Я хотел бы поблагодарить моего соавтора, Питера Торстейнсона (Peter Thorsteinson), за его руководство и помощь. Наконец, позвольте мне поблагодарить Всевышнего за то, что он предоставил мне такую возможность.

Мы хотели бы поблагодарить Эмили Фри (Emily Frey), Карен Гетман (Karen Gettman) и всех наших редакторов за их конструктивную помощь в усовершенствовании этой книги. Также мы хотели бы поблагодарить всех наших рецензентов за их детальные комментарии, которые во многом помогли обновить содержание книги.

Дж. Гнана Арун Ганеш (G. Gnana Arun Ganesh) является обладателем звания Microsoft .NET MVP (Most Valuable Professional – «наиболее ценный профессионал»), разработчиком, автором и консультантом по .NET. Также он ведет группу .NET Technology в Arun Micro Systems, которая занимается различными фазами технологии .NET. Он работал с технологией Microsoft .NET начиная с ее первоначальной бета-версии. Арун получил степень бакалавра электроники и коммуникационной техники в университете Бхаратьяра (Bharathiar), в колледже Kongo Engineering. Он является автором руководства .NET Reference Guide, опубликованного в InformIT. Он один из авторов Object Innovations (материалы для курса обучения фундаментальным программным технологиям). В качестве автора на темы .NET, он опубликовал более 50 статей о технологии .NET на различных Web-сайтах, посвященных этой теме. Как активный участник рецензирования в Prentice Hall, он написал множество технических рецензий, начиная с рецензии на книгу «C#: How to Program», написанную Харви и Полом Дейтел (Harry and Paul Deitel). Вот уже более двух лет, как администратор Arun Micro Systems, он обеспечивает онлайн-обучение .NET по всему миру.

4 июня 2003 года