

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

Оглавление

Предисловие	5
Глава 1. Криптография и безопасность в .NET	9
Природа этой книги	10
Опасность подстерегает повсюду	11
Природа криптографии и других средств обеспечения безопасности	14
Почему криптография и средства обеспечения безопасности так важны	14
Что возможно и что невозможно сделать с помощью криптографии и средств обеспечения безопасности	16
Безопасность в Windows: возраст зрелости	21
Среда разработки .NET Framework и «виртуальная машина» CRL	22
Как .NET Framework упрощает решение проблем безопасности	23
Надежность и платформа .NET Framework	24
Управляемый код и безопасность типов	24
Программирование с использованием криптографии в .NET	26
Программирование с использованием средств обеспечения безопасности в .NET	26
Безопасность, основанная на механизме ролей	27
CAS, свидетельства, политика и разрешения	27
Итоги главы	28
Глава 2. Основы криптографии	29
Чтобы секреты оставались секретами	30
Основные термины криптографии	30
Секретные ключи против секретных алгоритмов	33
Классические методы сохранения тайны	34
Рабочий фактор атаки методом «грубой силы»	53
Арифметика произвольной точности	54
Стеганография	55
Современные шифры	57
Криптография и .NET Framework	57
Симметричная криптография	58
Асимметричная криптография	59
Криптографические алгоритмы	62
Криптографические протоколы	66
Криптоаналитические атаки	68
Человеческий фактор	69

Риск и выигрыш	69
Другие важные концепции	70
Итоги главы	71
Глава 3. Симметричная криптография	72
Симметричные шифры	72
DES	74
Операционные режимы	75
«Тройной» DES	84
Rijndael	85
RC2	86
Программирование при помощи средств симметричной криптографии .NET	87
Основные криптографические классы	87
Класс SymmetricAlgorithm	88
Классы, производные от SymmetricAlgorithm	89
Примеры программирования с использованием симметричных алгоритмов	93
Криптографические потоки	97
Выбор надежных ключей	98
Проблемы передачи ключей	100
Шифрованные хеши и целостность сообщения	102
Хеш-алгоритмы с ключом и целостность сообщения	105
Итоги главы	106
Глава 4. Асимметричная криптография	107
Проблемы, связанные с использованием симметричных алгоритмов	107
Проблема распределения ключей	108
Проблема доверия	108
Идея асимметричной криптографии	109
Использование асимметричной криптографии	110
Аналогия с кодовым замком	111
Односторонняя функция с «черным ходом»	112
Преимущества асимметричного подхода	114
Сочетание асимметричных и симметричных алгоритмов	115
Существующие асимметричные алгоритмы	116
RSA: самый распространенный асимметричный алгоритм	117
Основания RSA	117
Миниатюрный пример RSA	119
Предостережение: вопросы вероятности	121
Программирование при помощи .NET Asymmetric Cryptography	123
Пример использования алгоритма RSA	123
Сохранение ключей в формате XML	129
Цифровые сертификаты	132
Итоги главы	132

Глава 5. Цифровая подпись	133
Хеш-алгоритмы	133
Характеристики хорошей хеш-функции	134
Хеш-алгоритмы, поддерживаемые в .NET	135
Класс HashAlgorithm	138
Классы MD5 и SHA	138
Класс KeyedHashAlgorithm	140
Идентификаторы объектов	140
Как работает цифровая подпись	141
RSA в качестве алгоритма цифровой подписи	143
Пример программы с использованием подписи RSA	144
Алгоритм цифровой подписи DSA	147
Математическое основание: теория групп	147
Задача о дискретных логарифмах	150
Как работает DSA	152
Иерархия класса AsymmetricAlgorithm	153
Класс DSACryptoServiceProvider	154
Пример программы с использованием DSA	154
Итоги главы	158
Глава 6. Криптография и XML	159
XML Encryption – шифрование XML	159
XML Encryption против SSL/TLS	160
Спецификация шифрования XML	161
Что обеспечивает шифрование XML	161
Синтаксис XML Encryption	162
Как работает шифрование XML	166
Классы, используемые в XML Encryption	167
Передача асимметричных ключей	171
Пример программы XmlEncryption	172
XML Signatures – подпись XML	184
Спецификация XML Signature	184
Что предусматривает спецификация XML Signature	185
Синтаксис XML Signature	185
Классы, используемые в XML Signatures	188
Программа EnvelopingXmlSignature	189
Сочетание XML Signing и XML Encryption	195
Итоги главы	196
Глава 7. Концепция безопасности, основанной на идентификации пользователей в .NET	197
Аутентификация и авторизация	198
Модель безопасности .NET	199
Администрирование безопасности на уровне Windows	200
Определение пользователей и ролей в Windows	201
Определение прав доступа к общей папке	201

Средства безопасности в NTFS	201
Администрирование безопасности на уровне .NET	205
Разрешения	206
Интерфейс IPermission	207
Иерархия наследования IPermission	208
Класс PrincipalPermission	209
Безопасность, основанная на идентификации пользователей	211
Объекты Principal и Identity	212
Интерфейс IIdentity	212
Классы, реализующие интерфейс IIdentity	212
Класс GenericIdentity	213
Класс WindowsIdentity	214
Объекты-принципалы	216
Интерфейс IPrincipal	217
Класс GenericPrincipal	218
Класс WindowsPrincipal	220
Два подхода к безопасности, основанной на идентификации пользователей	222
Императивный подход	222
Декларативный подход	229
Мандаты	231
Сетевые мандаты	232
Дисциплина безопасности	232
Принцип минимума полномочий	232
Раннее формулирование политики безопасности	233
Итоги главы	233
Глава 8. Доступ к коду в .NET	234
Необходимость в контроле доступа	234
Затраты против риска	235
Диапазон рисков	236
Степень доверия к сборке	238
Риски, связанные с обращением к традиционному коду	239
Безопасность, управляемый код и среда CLR	240
Промежуточный язык Microsoft	241
Верифицируемый код с контролем типов	241
Запросы разрешений	242
Использование CAS	243
Гибкий подход к обеспечению безопасности	243
Атака «с приманкой» и проход по стеку	244
Управление политиками безопасности при помощи групп кода	244
Основные концепции управления политиками безопасности	245
Использование средства конфигурирования .NET Framework Configuration	246
Использование утилиты Caspol.exe	260

Императивный и декларативный подходы в CAS	264
Концепция безопасности, основанная на свидетельствах	264
Класс Evidence	264
Получение свидетельства текущего домена приложения	268
Перечисление объектов Evidence	268
Пример программы WalkingThruEvidence	269
Доступ к WalkingThruEvidence через IIS	272
CAS в императивном стиле	274
Разрешения доступа кода	278
Производные классы CodeAccessPermission	278
Класс CodeAccessPermission	279
Класс UriIdentityPermission	283
Работа с разрешениями CAS	284
Декларативное разрешение доступа	290
Синтаксис объявления атрибутов с квадратными скобками	291
Атрибут Uri Identity Permission	292
Класс SecurityAction	293
Запросы разрешений	294
Пример программы PermissionRequest	294
Наборы разрешений	296
Класс PermissionSet	296
Определение набора разрешений при помощи конфигурационного файла	302
Итоги главы	306
Глава 9. ASP.NET	307
Базовые механизмы безопасности	308
Аутентификация: Кто вы?	308
Авторизация: Дозволен ли вам доступ к этому ресурсу?	308
Заимствование прав: Приложение действует от чьего-то имени	308
Реализация механизма аутентификации в ASP.NET	309
Конфигурация ASP.NET	310
Как устроена система конфигурирования ASP.NET и чем она хороша	311
Иерархия конфигурационных параметров	312
Описание	315
Аутентификация при помощи формы	318
Метод 1: хранение регистрационных данных в файле Web.config	319
Метод 2: хранение регистрационных данных в XML-файле	323
Файл Users.xml	323
Файл login.aspx	324
Метод 3: хранение регистрационных данных в базе данных	326
Классы для аутентификации при помощи форм	329
Аутентификация при помощи паспорта	331
Аутентификация Windows	338
Реализация авторизации ASP.NET	342

Авторизация на доступ к файлу	342
Авторизация на доступ к URL	343
Реализация заимствования прав ASP.NET	345
Итоги главы	345
Глава 10. Защита Web-служб	346
Основныe техники защиты Web-служб	347
Защищенное соединение	347
Аутентификация и авторизация	353
Механизмы аутентификации в протоколе HTTP	353
Аутентификация Web-служб при помощи заголовков SOAP	356
Архитектура сообщения SOAP	356
Создание прокси при помощи Visual Studio .NET	358
Технологии безопасности XML	360
Целостность	360
XML Signature	361
Защита данных и конфиденциальность	364
XML Encryption	364
Спецификация управления ключами XML (XKMS – XML Key Management Specification)	367
Язык разметки утверждений безопасности SAML (Security Assertion Markup Language)	367
Глобальная архитектура XML Web-служб (Global XML Web Services Architecture – GXA)	368
WS-Security	369
Начальная спецификация WS	371
Следующие шаги спецификаций	372
Почему WS-Security?	372
Распространение маркеров безопасности	373
Целостность сообщения	375
Конфиденциальность сообщения	376
Организации	385
Итоги главы	387
Приложение А. Пример атаки на код: перекрытие стека	388
Приложение В. Как работает шифр RSA	392
Модульная арифметика	392
Пример программы BigRSA	393
Пример программы CrackRSAWorkFactorDemo	396
Приложение С. Использование библиотеки GNU GMP	400
Установка Cygwin	400
Тестирование библиотеки Cygwin	405
Установка GMP	408
Удаление Cygwin из системы	411

Приложение D. Ресурсы по криптографии и безопасности	412
Общетеоретические и концептуальные книги	412
Книги по криптографической математике	413
Книги – руководства по безопасности	414
Популярные книги по криптографии	415
Группы новостей по криптографии	416
Полезные Web-сайты на темы криптографии и безопасности	416
Приложение E. Исследование Web-служб	418
Зачем нужны Web-службы	418
Определение Web-служб	420
Фундамент Web-служб	420
Следующее поколение распределенных вычислений: Web-службы	421
Преимущества Web-служб	422
Web-службы ASP.NET	422
Архитектура Web-служб	423
Модель кода для Web-службы	424
Разработка простой Web-службы	426
Concatenate.cs и Concatenate.asmx.cs	427
Директива @ WebService	431
Пространство имен System.Web.Services	432
Атрибут WebServiceAttribute	432
Класс WebService	433
Атрибут WebMethod	434
Управление сеансом	437
Протоколы	437
Доступ к Web-службе	438
Генерация прокси	438
Создание прокси-класса при помощи Wsdl.exe	439
Создание клиента Windows Form	440
Асинхронное программирование Web-служб	441
Два асинхронных метода (Begin и End)	442
Создание Web-службы ASP.NET «Калькулятор»	443
Web-службы все еще развиваются	446
Итоги	447
Предметный указатель	448