пользован для создания базы данных, которая хранит всю информацию (названия курсов, вопросы и ответы к ним), а также для хранения статистики о прохождении тестов. Все данные извлекаются из базы данных непосредственно во время тестирования, что обеспечивает сохранность данных. Вход в администраторскую часть осуществляется только после авторизации пользователя, во время которой происходит запрос пароля. JavaScript главным образом используется для отслеживания динамических событий и нажатий кнопок браузера. В системе также были использованы сессии cookies для хранения временных данных. Средой разработки PHP кода послужили UltraEdit и PHP Expert Editor.

Языком разработки был выбран именно PHP, т.к. он является одним из ведущих языков в своей области. Язык обеспечивает наиболее гибкое взаимодействие MySQL и веб-сервера. Обращения в SQL-базы данных производятся в PHP простыми командами, а возвращаемая информация обрабатывается достаточно легко. В сочетании с MySQL PHP обеспечивает сохранность и защищенность данных на хорошем уровне.

При разработке системы большое количество времени было потрачено не на разработку, а на сопровождение. На каждом этапе внедрения системы находились новые недочеты. Авторы доклада полагают, что для того, чтобы система широко использовалась, она должна иметь профессиональный дизайн, достаточное количество тестов (не менее 25) и не иметь ошибок при работе. Практическое решение этих задач потребовало значительных трудовых и временных затрат (более двух учебных семестров).

Литература:

1. Известия Белорусской инженерной академии. Научно-технический журнал, №1(19)/1 2005 г., с.93-95, 98-100.

2. С. Хайкин. Нейронные сети: полный курс – М.: «Вильямс», 2005. – 1104 с.

3. Д. Крейн, Э. Паскарелло, Д. Джеймс. Ajax в действии – М.: «Вильямс», 2006. – 640 с.

О ПРЕПОДАВАНИИ КУРСА «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ» В РАМКАХ СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Е.Н. Мельникова
Беларусь, г. Минск

Современная криптография – это обширная область знаний, сло-жившаяся в результате интенсивных исследований последних тридцати лет. Одним из важных аспектов этой области являются крипто-графические протоколы.

Криптографические протоколы представляют собой необходимый элемент распределенных систем и играют ключевую роль в процессе передачи информации через открытые сети, такие как Интернет. Эти сети являются небезопасными в том смысле, что любой нарушитель с соответствующими техническими возможностями может контролировать и даже модифицировать сообщения, пе-

редаваемые по сети. Криптографические протоколы и используют для того, чтобы обеспечить защищенное взаимодействие конечных пользователей по незащищенным каналам связи. Большинство криптографических протоколов в своей основе используют криптографические алгоритмы шифрования, выработки цифровой подписи, вычисления кода аутентификации сообщений и хэширования.

Учитывая важность раздела современной криптографической науки, посвященного изучению криптографических протоколов, в Белорусском государственном университете на факультете прикладной математики и информатики с 2006 года для студентов пятого курса специальности «Компьютерная безопасность», имеющих специализацию «Математические методы защиты информации», введен специальный курс «Криптографические протоколы», рассчитанный на 34 лекционных часа. Этот курс основывается на знаниях студентов, полученных при изучении таких общих курсов, как «Криптографические методы», «Теоретические основы компьютерной безопасности», «Системы и сети передачи информации», и поддерживается спецлабораторией «Безопасность информационных технологий».

Цель спецкурса «Криптографические протоколы» состоит в том, чтобы изложить основные принципы разработки, анализа, реализации и применения криптографических протоколов для обеспечения безопасности в современных информационных системах и сетях, сделав акцент на Международных стандартах. При подготовке спецкурса была использована литература, представленная в [1-9], а также опыт автора, полученный при выполнении научных работ по соответствующей тематике.

На сегодняшний день основными задачами, которые решаются с помощью криптографических протоколов в компьютерных сетях передачи данных, являются следующие:

1. Первостепенная задача – это установление подлинности сторон, участвующих в протоколе. Типичными участниками протоколов могут быть пользователи, рабочие станции, выполняемые от имени пользователей процессы и пр. Процедуру доказательства подлинности в распределенных системах называют аутентификацией, и реализуется она с помощью протоколов аутентификации.

2. Многие протоколы аутентификации, однако, также используются и для решения второй задачи: распределение между участниками протокола секретного сеансового ключа для дальнейшего защищенного взаимодействия. Хотя успешное выполнение протокола аутентификации и обеспечивает подлинность участников, но оно не гарантирует подлинность и конфиденциальность любого последующего взаимодействия. Для защищенного взаимодействия в будущем, в процессе аутентификации или сразу же после него, должен быть распределен секретный сеансовый ключ. Это распределение обеспечивается протоколами распределения ключевой информации.

В связи с вышесказанным, курс «Криптографические протоколы» условно разбит на две части: «Криптографические протоколы аутен-тификации» и «Криптографические протоколы распределения ключей».

Задачей преподавания дисциплины «Криптографические протоколы аутентификации» является изучение различных методов аутентификации, основных схем и конструкций протоколов, включая схемы и конструкции протоколов, использованные в Международных стандартах и описанные в литературе, а также изучение теоретических аспектов создания, применения и анализа стойкости криптографических протоколов аутентификации.

В этой части спецкурса рассматриваются следующие основные темы:

1. Введение в теорию криптографических протоколов. Здесь рассматриваются такие вопросы, как предмет и цель спецкурса, актуальность задач построения, использования и анализа криптографических протоколов в целом. Устанавливаются правила описания компонентов криптографического протокола и соглашения о смысле протокольных сообщений и их синтаксической структуре.

2. Криптографические протоколы: общие положения. В рамках этой темы дается определение тому, что понимается вообще под протоколом и, в частности, под криптографическим протоколом, рассматриваются задачи, решаемые с помощью криптографических протоколов. Описываются стандартные механизмы, позволяющие установить подлинность сеанса связи, к числу которых относятся механизмы, использующие такие параметры, как случайные числа, временные отметки и порядковые номера. Рассматриваются базовые схемы использования этих параметров в криптографических протоколах.

3. Протоколы аутентификации. Это основная тема первой части спецкурса. В ней дается определение понятий идентификация и аутентификация, рассматриваются основные методы аутентификации: простая и строгая аутентификация, взаимная и односторонняя аутентификация, аутентификация с привлечением доверенной стороны. Далее приводится описание и анализ целого ряда протоколов аутентификации, к числу которых относятся: протоколы аутентификации, основанные на пароле пользователя и функции хэширования; протоколы односторонней и взаимной аутентификации стандарта ISO/IEC 99798-2, основанные на симметричном алгоритме шифрования, и протоколы стандарта ISO/IEC 99798-4, основанные на MAC-коде. Эти стандарты приняты Международной организацией по стандартизации (International Organization for Standardization – ISO) и Международной электротехнической комиссией (International Electrotechnical Commission – IEC).

4. Типичные атаки на криптографические протоколы. В рамках этой темы дается определение того, что понимается под атакой на криптографический протокол: успешная атака на протокол обычно не связана со взломом криптографического алгоритма. Наоборот, как правило, атака становится возможной вследствие ошибок, сделанных при разработке протокола, а не криптографического алгоритма. Поэтому здесь рассматриваются несколько хорошо известных видов атаки и приводятся примеры протоколов, недостатки которых позволяют провести тот или иной вид атаки.

Задачей преподавания дисциплины «Криптографические протоколы распределения ключей» является изучение различных протоколов распределения и управления ключевой информацией с использованием и без использования до-

веренной стороны, включая протоколы из Международных стандартов, а также изучение теоретических аспектов создания, применения и анализа стойкости криптографических протоколов распределения ключей. Эта дисциплина особенно актуальна, поскольку одной из главных трудностей, возникающих при построении криптографической системы защиты в компьютерных сетях, как раз и является распределение ключевой информации.

Эта часть спецкурса включает следующие темы:

1. Ключевая информация. Тема посвящена очень важному ком-поненту в организации защищенного взаимодействия – крипто-графическим ключам. Здесь рассматриваются типы ключей по их практическому использованию: главные ключи, ключи шифрования ключей, ключи шифрования данных. Дается определение криптопериода ключа и классификация ключей по криптопериоду: долговременные ключи, кратковременные и сеансовые ключи. Определяются взаимосвязи между типами ключей. Также в этой теме рассматриваются способы распределения ключей: централизованное (с участием доверенной стороны) и децентрализованное (прямой обмен), и приводится классификация способов распределения.

2. Инфраструктура открытых ключей. В этой теме даются основные понятия и определения связанные с инфраструктурой открытых ключей, приводится структура сертификата и список отозванных сертификатов по стандарту X.509, форматы данных по стандарту PKCS#7.

3. Протоколы распределения ключей, основанные на симметричной криптосистеме. В рамках этой темы рассматривается две группы протоколов. Первую группу составляют двухсторонние протоколы распределения ключей, не использующие доверенную сторону. К ним относятся: протокол, использующий необратимую функцию, двухсторонний протокол распределения сеансового ключа с использованием MAC-кода, протоколы стандартов ISO/IEC 9798-2 и ISO/IEC 11770-2. Во вторую группу входят протоколы распределения ключей с участием доверенной стороны. К ним относятся известные из литературы протоколы: Нидхема-Шредера, Деннинга-Сакко, Отвея-Рииса, Неймана-Стаблбайна, трехсторонний протокол, основанный на MAC-коде, а также ряд протоколов стандартов ISO/IEC 9798-2 и ISO/IEC 11770-2. Для всех протоколов приводится структурная схема, дается их описание и анализ стойкости.

4. Протоколы распределения ключей, основанные на асимметричной криптосистеме. Тема знакомит с некоторыми протоколами, использующими асимметричную криптосистему. Это протокол Диффи-Хеллмана установления общего ключа, протокол STS (станция к станции) установления общего ключа, протокол взаимной аутентификации Нидхема-Шредера с участием доверенной стороны, протокол распределения ключей Деннинга-Сакко с участием доверенной стороны. Для всех протоколов приводится структурная схема, дается их описание и анализ стойкости.

5. Криптографические протоколы, используемые на практике. Здесь дается краткий обзор таких практических протоколов, как протокол аутентификации NTLM, протокол аутентификации и распределения ключей Kerberos, протокол SSL(TLS) и протокол обеспечения безопасности в Интернет IPSec.

Следует отметить, что раздел криптографии, посвященный криптографическим протоколам, очень обширный и многогранный. Естественно, многие темы не вошли в предложенный курс, поэтому имеется возможность материал курса обновлять и перерабатывать.

Выражаю благодарность заведующему кафедрой математического моделирования и анализа данных Белгосуниверситета Ю.С. Харину за предоставленную возможность прочитать разработанный курс для студентов, специализирующихся в области компьютерной безопасности.

Литература

1. Мао В. Современная криптография: теория и практика. Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768 с.

2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты информации. – М.: ДМК, 2000. – 448 с.

3. Смит Р.Э. Аутентификация: от паролей до открытых ключей. Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 432 с.

4. Соколов А.В., Шаньгин В.Ф. Защита информации в распре- деленных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

5. Столлингс В. Криптография и защита сетей: принципы и практика. Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 564 с.

6. Clark J., Jacob J. A survey of authentication protocol literature: version 1.0, 1997. Avail. at www.cs.york.ac.uk/jac/papers/drareview.ps.gz.

7. ISO/IEC 9798-2. Information technology – Security techniques – Entity authentication. Part 2: Mechanisms using symmetric encipherment algorithms. International Standard, 1999-07-15.

8. ISO/IEC 9798-4. Information technology – Security techniques – Entity authentication. Part 4: Mechanisms using a cryptographic check function. International Standard, 1999-12-15.

9. ISO/IEC 11770-2. Information technology – Security techniques – Key management. Part 2: Mechanisms using symmetric techniques. International Standard, 1996-06-01.

ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО СОЗДАНИЯ ЭЛЕКТРОННЫХ УЧЕБНИКОВ

С.В. Леончик
Беларусь, г. Гродно

В настоящее время активно разрабатываются компьютерные средства для ведения учебных курсов. Практически по всем направлениям учебных дисциплин создаются электронные учебники и самоучители. Усиление интереса к подобным источникам связано с возможностью повышения качества образования за счет использования информационно-коммуникационных технологий в системе образования. Использование электронных учебников позволяет повысить роль управляемой самостоятельной работы студентов, обеспечить качество об-