аутентификация, без нее нет возможности ограничить доступ пользователей к конкретным информационным ресурсами.

Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли. Этот способ аутентификации получил самое широкое распространение. Главные достоинства парольной аутентификации – простота и привычность.

Сегодня количество программных продуктов, используемых в любой компании, довольно велико. И можно с уверенностью сказать, что существует тенденция увеличения их количества, причем независимо от профиля компании.

Многие из используемых приложений требуют прохождения аутентификации, то есть указания логина и пароля пользователя. При этом с точки зрения пользователей, при использовании паролей возникают следующие проблемы: возрастает как число используемых паролей, так и их сложность, с определенной периодичностью пароли необходимо менять.

Для облегчения процесса парольной аутентификации многие пользователи прибегают к таким мерам, как использование простых паролей, использование одного пароля во множестве приложений, запись паролей на стикерах или использование в качестве пароля какого-то символа, находящегося в пределах их рабочего места (модель монитора, например). В результате этих действий уровень информационной защищенности компании значительно понижается.

В работе рассматриваются методики оптимизации системы аутентификации пользователей. Проведен обзор и анализ существующих механизмов аутентификации, рассмотрены способы оценки эффективности механизмов аутентификации, а также исследованы результаты оптимизации существующих механизмов аутентификации в корпоративной сети предприятия.

СИСТЕМА РАСПРЕДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ ПОСРЕДСТВОМ PEER-TO-PEER СЕТИ

Е.В. Разумов

В информационном обществе главным ресурсом является информация. В данный момент большая часть информации хранится и передается в цифровом виде. При этом важным аспектом является хранение, а также передача конфиденциальной информации.

В настоящее время существует множество различных способов обеспечения безопасной пересылки данных. И наиболее распространенным из них является способ, основанный на использовании протоколов SSL [1] и его модификации TLS. Однако при этом существует ряд атак, которые применимы даже для SSL соединения. Одной из них является так называемая MITM-атака (man in the middle). Она подразумевает наличие атакующего, который способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале.

Одним из возможных методов, по средствам которого можно достичь большую устойчивость к MITM-атакам, является метод построения системы распределенной передачи данных посредством peer-to-peer сети. Основная идея, заложенная в данную систему, заключается в разбиении передаваемой информации на блоки, шифровании каждого из этих блоков и последующей передаче их через отдельный промежуточный узел. Размер блоков и их количество может быть выбрано произвольно. От этих параметров будет зависеть число участвующих в передаче узлов сети и, соответственно, скорость передачи. В передаче необходимой информации могут участвовать не все узлы, в то время как некоторые узлы могут участвовать в этом более одного раза.

Таким образом разработанная модель решает проблему перехвата сообщения целиком, так как злоумышленник не может изначально знать через какие узлы будут передаваться части сообщения, а внедриться между всему участвующими узлами сети при достаточно большом количестве этих узлов практически не представляется возможным. К тому же даже перехват

одной или более частей сообщения (но не всех) и ее расшифровывание не дает возможности получить все сообщение целиком.

Литература

1. Freier A. The Secure Sockets Layer (SSL) Protocol Version 3.0 – August 2011.

МОДЕЛИРОВАНИЕ АКУСТИЧЕСКИХ ЗАДАЧ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО СРЕДСТВА

И.В.Савченко

Одним из подходов к решению проблема защиты речевой информации от утечек по акустическому каналу является разработка базовой программной модели, которая основана на адаптации физической модели под программную реализацию. Для разработки программного средства определены входные и выходные параметры базовой физической модели, критерии выбора среды разработки и непосредственно сама среда разработки программного средства, а также предложена архитектура программного средства.

Входные величины и параметры, которыми будет оперировать разрабатываемая программная реализация акустической модели, основываются на наборе математических формул и уравнений акустики, описывающих физические процессы в рамках заданного класса акустических задач.

С учетом требований к программной реализации и исследуемой физической модели, оптимальным языком программирования является Java, позволяющий создавать программы в соответствии с концепциями объектно-ориентированного программирования в рамках распространенных паттернов проектирования.

Архитектура программного средства представлена в виде набора шаблонов проектирования, оптимальным из которых является шаблон проектирования «Мост». При реализации базовой архитектуры приложения через шаблон «Мост», изменение структуры интерфейса не мешает изменению структуры реализации.

На основании разработанной архитектуры реализован прототип программного средства, демонстрирующий работу описанного выше алгоритма в рамках выбранной математической модели. В качестве входных параметров заданы: размер помещения и взаимное расположение стен; источник звука, являющийся центром исходящих лучей; точность расчета, включающая в себя количество лучей и количество отражений. Чтобы иттерационно продемонстрировать принцип работы алгоритма, при работе с программой изменялись значения, определяющие точность заданных параметров.

ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ВЕКТОРНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ ХРАНЕНИЯ ИНФОРМАЦИИ

С.Б. Саломатин, Т.А. Андриянова

Распределенные системы хранения информации широко используются в современных инфокоммуникационных системах. При этом появляется возможность использовать пространственно-временную избыточность распределенных систем для защиты информации.

Один из методов защиты данных может быть основан на схеме разделения секрета среди группы пользователей (агентов) распределенной информационной сети.

Векторная пороговая схема, использующая геометрию точек в пространстве.

Сообщение определяется как точка в n-мерном пространстве. Каждое уравнение в пороговой схеме – это уравнение $(n-1)-$ мерной гиперплоскости, содержащей эту точку.

Защищаемые массивы данных, разбиваются на несколько отображений. Коэффициенты отображений выбираются случайным образом из множества целых чисел меньших модуля p или используются элементы массива данных. Матричное представление