Иванова и др.; под ред. А. В. Бриллиантова. - М.: Проспект, 2010. - 1392 с.
4. Приговор Кристоферу Чейни вынесен [Электронный ресурс]. URL: http://www.xakep.ru/magazine/xa/169/xa_169.pdf (дата обращения: 07.04.2014).
5. Гендиректор осуждена за переписку "ВКонтакте" [Электронный ресурс]. URL: http://pravo.ru/news/view/47465/ (дата обращения: 03.04.2014).
6. Кадников, Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни / Б.Н. Кадников; под. ред. Н.Г. Кадникова. - М.: Юриспруденция, 2011. - 136 с.

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ В СТУДЕНЧЕСКОЙ ИНТЕРАКТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

А.Т. Эдокова, АлтГУ, физико-технический факультет, 1 к.
Научный руководитель – ***В.В. Белозерских,***
старший преподаватель.

Период конца XX – начала XXI века ознаменовался бурным развитием информационных технологий. На сегодняшний день нет ни одной области человеческой деятельности, где они не нашли бы свое применение. Информация сегодня - средство обеспечения успеха в бизнесе и поэтому является объектом основательного контроля. К сожалению, интерес к взлому или несанкционированному использованию информационных систем постоянно растет, и поэтому требуются серьезная многоуровневая защита. Существенно вырастает цена, которую приходится платить правообладателю информации, не предпринимающему должных усилий по защите своих тайн.

Поэтому сегодня, для того чтобы данные не были уничтожены или модифицированы несанкционированным образом нужно решать различные проблемы их защиты. Одним из путей решения этих проблем является использование аутентификации, на рассмотрении которой остановимся подробнее на примере студенческой интерактивной информационной системы.

Немного расскажем о самой системе. С точки зрения пользователя клиентский терминал представляет из себя LCD панель

на которую выводится информация. Панель установлена таким образом, чтобы исключить прямой физический контакт между пользователями и системой. Их взаимодействие осуществляется с помощью жестов, посредством обработки изображений с видеокамеры. Для реализации этих возможностей, в качестве клиентского устройства используется микрокомпьютер RPi. Raspberry Pi это компактный микрокомпьютер размером с банковскую карту. Данный микрокомпьютер имеет 512 Мб ОЗУ и 700 МГц ARM процессор и имеет производительность на уровне Pentium III – 600 МГц. Может работать под многими ОС, включая те, что основаны на ядре Linux.

Что касается реализации всей системы, то она выполнена на 3-х уровневой клиент-серверной архитектуре, с использованием собственной виртуальной сети.

Рис.1. Упрощенная схема информационной системы.

Пересылка данных от сервера клиенту предполагает передачу с использованием протоколов TCP/UDP, но с формированием собственных криптографически защищеных пакетов, с целью ограничения внешнего доступа злоумышленников к системе и нарушения её нормального функционирования.

Основными механизмами защиты информации предлагается аутентификация (установление подлинности) и шифрование.

Аутентификацию можно разделить на два вида: аутентификацию пользователя и аутентификацию источника данных.

В данной работе рассмотрен только механизм аутентификации пользователя.

Подсистема аутентификации пользователей — важнейший компонент системы информационной безопасности, и ее значение трудно переоценить. Подсистема аутентификации подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа. [1] Парольная аутентификация (при попытке входа в сеть пользователь набирает свой пароль) является самой экономичной по стоимости, она проста и привычна. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Пароль пользователя можно подсмотреть, перехватить в канале связи, да и просто подобрать. В связи с этим, следует признать, что в нашем случае парольная аутентификация является ненадежной. [2]

Поэтому предлагается реализовать аутентификацию пользователя с помощью метода, предложенного Массачусетским технологическим институтом в середине 80-х годов.

В нашем случае сеть - открытая (незащищенная), в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные системы. Суть метода в том, что каждый субъект обладает секретным ключом. Субъектами в данной системе будут являться клиент (пользователь) – обозначим его К, и сервер – обозначим его С. Чтобы клиент К мог доказать свою подлинность серверу С, он должен не только назвать себя, но и продемонстрировать знание секретного ключа. К не может просто послать С свой секретный ключ, во-первых, потому, что сеть открыта, а, во-вторых, потому, что С не знает (и не должен знать) секретный ключ К. В связи с этим требуется создать доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. Обозначим третью сторону как А.

Чтобы с помощью А получить доступ к С, К посылает А запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ А возвращает так называемый билет, зашифрован-

ный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента.

Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом.

Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные, то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. [3]

Проиллюстрируем описанную процедуру.

Рис.2. Упрощенная схема предложенного метода аутентификации пользователя.

Так как компонентов сети немного, то создание доверенной стороны А сопряжено с определенными затратами. Для решения этой проблемы нужен дополнительный компонент, например, еще один ПК, который должен работать не прерывно для обеспечения процесса аутентификации. Это и является своеобразной издержкой предложенного механизма аутентификации.

Рис.3. Упрощенная схема информационной системы, которая получится в результате.

Таким образом, можно с большой долей уверенности утверждать, что представленный в работе метод является приемлемым для данной информационной системы, хотя и не лишен определенных издержек.

Список литературы

1. Голов А., Прудников И. Аутентификация пользователей – современные методы // CIO. 2006. №4(93). С. 30-31.
2. Алферов А. П., Зубов А. Ю. Основы криптографии: учебное пособие. Москва: Гелиос АРВ, 2002. - 332 с.
3. Вьюкова Н., Сервер аутентификации Kerberos [Электронный ресурс] – Режим доступа: http://www.osp.ru/os/1996/01/178793/, свободный. – Загл. с экрана

ПРИМЕНЕНИЕ ФУНКЦИЙ УОЛША ДЛЯ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ГАРМОНИЧЕСКИХ СИГНАЛОВ ПРИ НАЛИЧИИ СЛУЧАЙНОЙ ПОМЕХИ В СЕЛЕКТИВНЫХ ПОИСКОВЫХ СИСТЕМАХ

А.В. Герусов, АлтГУ, физико-технический факультет, 5к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Рост числа объектов информатизации, обрабатывающих и содержащих конфиденциальные данные, ставит жесткие требования к комплексному подходу обеспечения информационной безопасности. Важную роль в решении этой задачи играют различные