КРАТКИЕ СООБЩЕНИЯ

УДК 681.586'33, 681.5.015.87

НЕЯВНЫЙ МАСКАРАДИНГ ПРИ ДОСТУПЕ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СЕТИ

И.И. Прокопов

IMPLIED MASQUERADING AT CONFIDENTIAL INFORMATION ACCESS IN COMPUTER NETWORK

I.I. Prokopov

Рассмотрены способы и причины неявного доступа к данным в отсутствие владельца ключа. Представлена модель неявного доступа в виде матрицы доступа. Предложены способы противодействия подмене (маскарадингу) оператора.

Ключевые слова: неявный доступ, конфиденциальные данные, маскарадинг.

Methods and reasons for implied data access at the absence of the key carrier are considered in the article. Implied access model in the form of an authorization matrix is given. Methods for countering substitution of an operator (that is masquerading) are suggested.

Keywords: implied access, confidential information, masquerading.

При доступе к конфиденциальным данным через компьютерную сеть по клиент-серверной схеме используются авторизованные рабочие станции. Можно рассматривать такую локальную сеть как открытую распределенную среду, в которой пользователи со своих рабочих станций должны иметь возможность доступа к услугам на серверах в сети [1]. К серверам должны получать доступ только зарегистрированные пользователи и сервер должен иметь возможность аутентифицировать запросы к сервисам. Пользователи (операторы) используют на рабочем месте электронные ключи для шифрования данных. В совокупности это дает надежный авторизованный доступ к данным, не предполагающий утечку информации к другим лицам. Но в ряде случаев возможен неявный доступ в отсутствие владельца ключа.

Способы и причины неявного доступа к данным

Под неявным доступом понимается доступ к данным неавторизованным оператором (т. е. не имеющим на это право).

Способы неявного доступа:

1. Доступ к данным неавторизованным оператором с авторизованной рабочей станции с использованием ключей шифрования, хранящихся на съемном носителе этой рабочей станции.

2. Доступ к данным неавторизованным оператором с неавторизованной рабочей станции с использованием копий ключей шифрования, хранящихся на съемном носителе этой рабочей станции. При этом способе требуется подделка аппаратных характеристик другой рабочей станции для целей ее авторизации на сервере в качестве легальной. При этом требуются ключи шифрования (копии) с оригинальной рабочей станции, не имеющие привязки к оборудованию и носителю, либо оригинальный носитель. Рабочая станция расположена в локальной сети сервера.

3. Вход на авторизованную рабочую станцию с другой ЭВМ посредством программ удаленного доступа (администрирования), в том числе из сети Интернет. Ключи шифрования должны быть в наличии на оригинальном носителе (в случае аппаратной привязки) и подключены к ЭВМ. Доступ осуществляется с легальной рабочей станции и с оригинальными ключами. Доступ возможен и в рабочее время при отсутствии оператора.

Рассмотрим причины и условия, приводящие к неявному доступу.

1. Наличие подключенных оригинальных носителей ключей включенной рабочей станции при отсутствии авторизованного оператора на ра-

Прокопов Игорь Игоревич – доцент кафедры цифровых радиотехнических систем, Южно-Уральский государственный университет; crts@drts.susu.ac.ru

Prokopov Igor Igorevich – associate professor of the Department of Digital Electronic Systems, South Ural State University; crts@drts.susu.ac.ru

Модель неявного доступа

		Время		Тип оператора		Тип рабочей станции	
		раб.	нераб.	авт.	неавт.	авт.	неавт.
Время	раб.	–	–	X	0	X	1
	нераб.	–	–	0	X	0	X
Тип оператора	авт.	X	0	–	–	X	0
	неавт.	0	X	–	–	1	X
Тип рабочей станции	авт.	X	0	X	1	–	–
	неавт.	1	X	0	X	–	–

бочем месте. В этом случае возможен доступ как удаленным способом, так и с консоли.

2. Наличие питания 220 В на рабочей станции в нерабочее время. В связи с наличием в современных аппаратных платформах средств удаленного администрирования посредством программного обеспечения BIOS компьютер может быть включен удаленно через сеть. В ряде случаев компьютеры не выключаются вообще для целей их администрирования (архивирование данных, резервное копирование, установка обновлений и ПО и т. п.). Если в помещение нет физического доступа, компьютер может быть использован для доступа через удаленный рабочий стол или терминальную программу.

Разделим условно все общеупотребимые виды ключей на две категории:

А. С привязкой к носителю. Простое копирование файлов с такого носителя либо невозможно (смарт карты), либо бессмысленно, так как при смене носителя требуется перегенерация ключей при наличии оригинального носителя.

Б. «Плавающие» ключи. Требуется всего лишь наличие соответствующих файлов по пути, указанному в драйверах доступа. Наиболее удобный для злоумышленника тип, так как копирование возможно по сети.

В некоторых организациях, имеющих клиентские части от 5–10 банков, образуется смесь всех возможных типов ключей, каждый из которых имеет свой носитель, включая ключи категории Б.

Основное условие, определяющее возможность реализации всех способов доступа, – это наличие носителей закрытых ключей шифрования в соответствующих портах ЭВМ при отсутствии оператора, а также наличие у неавторизованного оператора кода для идентификации владельца ключа (PIN-код). Этот код можно получить с помощью аппаратных или программных кейлогеров [2].

Модель неявного доступа

Модель неявного доступа представлена в виде матрицы доступа (см. таблицу). Операторы и рабочие станции разделены на два типа – авторизованные и неавторизованные. Символ «X» означает возможность доступа к данным, «0» – отсутствие доступа к данным (с консоли), «1» – доступ к данным при особых условиях (например, физическое отсутствие авторизованного оператора). Параметр «время» имеет значения «рабочее» и «нерабочее».

Способы противодействия подмене (маскарадингу) оператора

1. Применение «тонких» клиентов-терминалов для доступа к данным с целью исключения программных кейлогеров и удаленного администрирования, предполагая при этом надежность администратора сервера баз данных и сервера аутентификации [1].

2. Запрет администрирования рабочей станции через сеть (только локальное администрирование), в особенности через сеть Интернет.

3. Изоляция авторизованной рабочей станции от других узлов локальной сети программно-аппаратными средствами [3].

4. Контроль наличия съемных носителей (и параллельно аппаратных кейлогеров) при покидании рабочего места, выключении ЭВМ. Возможно использование радиометок (RFID) для носителей ключей (при привязке ключей к носителю).

Литература

1. Столлингс, В. Криптография и защита сетей: принципы и практика: пер. с англ. / В. Столлингс. – 2-е изд. – М.: Издат. дом «Вильямс», 2001. – 672 с.

2. Хорев, А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1: Технические каналы утечки информации / А.А. Хорев. – М.: НПЦ «Аналитика», 2008. – 436 с.

3. Брэгг, Р. Безопасность сетей. Полное руководство: пер. с англ. / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М.: Изд-во «ЭКОМ», 2006. – 912 с.

Поступила в редакцию 30 мая 2012 г.