УДК 681.32

**Д.А. Бортник, Е.Л. Кротова**

Пермский национальный исследовательский политехнический университет, Пермь, Россия

# НАСТРОЙКА БЕЗОПАСНОГО УДАЛЕННОГО УПРАВЛЕНИЯ МАРШРУТИЗАТОРОМ CISCO С ПОМОЩЬЮ ПРОТОКОЛА SSH

Компьютерные сети появились относительно недавно, и в настоящее время трудно представить себе организацию, которая не имеет выхода в Интернет или в которой нет собственной корпоративной сети. Для управления сетью необходимо настраивать сетевое оборудование и поддерживать его работоспособность. Одним из способов, наиболее распространенным в последнее время, является удаленное управление, осуществляемое посредством различных протоколов.

В статье обосновывается актуальность удаленного управления оборудованием. Приведены данные аналитических агентств об использовании сетевого оборудования в мире. Указаны особенности протокола SSH, его назначение и существующие версии. Перечислены основные компоненты и раскрыта их роль в структуре протокола. В статье также можно найти информацию о надежности протокола с точки зрения криптоанализа, об используемых принципах шифрования и о выборе ключей. Рассмотрена процедура аутентификации сервера, указаны угрозы, которые могут возникнуть при отключении проверки соответствия сервера и используемого ключа. Приведены способы аутентификации клиентов: аутентификация с использованием открытых ключей, парольная аутентификация и аутентификация по хостам. У каждого способа рассмотрены существующие недостатки. Указана минимальная версия операционной системы маршрутизатора Cisco, позволяющая использовать протокол SSH. Приведены настройки маршрутизатора, необходимые для работы протокола, описано назначение каждого этапа настройки. В конце статьи обосновывается необходимость мониторинга работы сети. Анализируется трафик между хостом и маршрутизатором с помощью программы Wireshark. Приведены схема сети, используемая для анализа, IP-адреса оборудования и результаты захвата трафика.

**Ключевые слова:** удаленное управление, SSH, Cisco, анализ трафика, Wireshark.

**D.A. Bortnik, E.L. Krotova**

Perm National Research Polytechnic University, Perm, Russian Federation

# CONFIGURATION OF CISCO ROUTER FOR SECURE REMOTE CONTROL USING SSH PROTOCOL

Computer networks have appeared rather recently and nowadays it’s hard to imagine an organization which don’t have the Internet connection or don’t have its own corporate network. It is necessary to configure network equipment and maintain its operability for network control. The most widespread way is remote control, implemented by means of various protocols.

At the article it was proved the relevance of equipment remote control. It was shown the data of analytical agencies about using of network equipment in the world. It was listed features of the SSH

protocol, its purpose and available versions. It was listed the main components and disclosed their meanings in the SSH's structure. At the article you can also find the information about reliability of the SSH protocol in terms of cryptoanalysis, the information about encryption principles and key selection. It was considered the server authentication procedure, listed main threats can occur when you shutdown compliance check between the server and used key. It was shown three ways of clients authentication: authentication with public keys, password authentication and host authentication. It was considered main limitations of each way. It was listed the minimal version of Cisco router's IOS allowing to use the SSH protocol. It was listed necessary for protocol functioning router's settings and described the purpose of each setting stage. In conclusion it was proved the necessity of network monitoring and analyzed traffic between host and router using Wireshark. It was listed the network scheme, IP-addresses of equipment and traffic capturing results.

**Keywords**: remote control, SSH, Cisco, traffic analysis, Wireshark.

**Введение.** В настоящее время наблюдается быстрое развитие вычислительных сетей. Появилось большое количество разнообразного коммуникационного оборудования – коммутаторы, маршрутизаторы, шлюзы. Благодаря такому оборудованию появилась возможность построения больших корпоративных сетей, насчитывающих тысячи компьютеров и имеющих сложную структуру [1]. Непосредственная настройка и обслуживание большой сети могут занимать достаточно много времени, отсюда возникает необходимость удаленного управления оборудованием.

Одним из протоколов дистанционного управления компьютером является SSH. Этот протокол отличается высокой защищенностью за счет поддержки криптостойких алгоритмов и ряда дополнительных возможностей [2].

По данным аналитических агентств, производителем наиболее популярного оборудования коммутации и маршрутизации для средних и крупных предприятий является Cisco Systems (около 64 % мирового рынка) [3]. Исходя из этого, в статье рассматривается настройка маршрутизаторов именно компании Cisco Systems.

**1. Описание протокола Secure Shell (SSH).** Спецификация протокола SSH содержится в документе RFC 4251 [4, 5], опубликованном в январе 2006 года.

SSH используется для безопасного удаленного входа в систему и для организации других безопасных служб через незащищенные сети. Протокол состоит из трех основных составляющих:

– протокол транспортного уровня (SSH-TRANS). Обеспечивает аутентификацию сервера, конфиденциальность и целостность. Также может обеспечивать сжатие данных. Протокол обычно работает через соединение TCP/IP, но может использоваться поверх любого другого протокола с гарантированной доставкой данных;

– протокол аутентификации пользователей (SSH-USERAUTH). Аутентифицирует пользователей, подключающихся к серверу. Работает поверх (SSH-TRANS);

– протокол соединения (SSH-CONNECT). Мультиплексирует шифрованный туннель в несколько логических каналов. Работает поверх (SSH-USERAUTH).

Основной задачей протокола SSH является повышение уровня безопасности в Интернете. Протокол пытается сделать это за счет обеспечения максимальной простоты, даже допуская некоторое снижение уровня безопасности.

Особенности алгоритмов шифрования, используемых в протоколе SSH:

– все алгоритмы шифрования, обеспечения целостности и генерации открытых ключей являются широко известными и проверенными;

– все алгоритмы используются с криптографически обоснованным размером ключей, который позволяет надеяться на обеспечение защиты от самых мощных криптоаналитических атак в течение десятилетий;

– все алгоритмы согласуются, и в тех случаях, когда тот или иной алгоритм не поддерживается, обеспечивается простой переход к использованию другого алгоритма без изменения базового протокола.

Для аутентификации каждому серверному хосту следует иметь ключ хоста. Хосты могут иметь множество ключей, созданных с использованием различных алгоритмов. Также возможно использование ключа несколькими хостами.

Ключ сервера используется в процессе обмена ключами для подтверждения того, что клиент действительно связывается с нужным сервером. Чтобы такая проверка была возможной, клиент должен заранее знать открытый ключ сервера.

Протокол позволяет отключить проверку соответствия «сервер – ключ» при первом подключении к хосту. Это позволяет подключиться к хосту до получения от него ключа или сертификата. Такой подход обеспечивает защиту от пассивного прослушивания канала, но существует уязвимость активных атак со стороны злоумышленника. При реализации протокола следует предпринимать разумные меры по проверке ключей хостов. Примером возможной стратегии может служить следующая: принятие ключа без проверки только при первом соедине-

нии с хостом, сохранение полученного ключа в локальной базе данных и его использование при каждом последующем подключении к данному хосту.

Предполагается, что в некоторых случаях протокол будет использоваться без предварительной достоверности связи между ключом и именем хоста. Такое использование уязвимо для man-in-the-middle атак.

На рис. 1 схематично изображена атака типа man-in-the-middle при взаимодействии клиента и сервера (назовем их Алиса и Боб) с участием злоумышленника (Труди). Каждое сообщение, посылаемое Алисой в шифрованном сеансе, перехватывается Труди, сохраняется, изменяется, если это нужно, и отправляется Бобу. То же самое происходит в обратном направлении. Труди видит все сообщения и может изменять их по своему усмотрению, в то время как Алиса и Боб полагают, что у них имеется защищенный канал для связи друг с другом [6].


Рис. 1. Атака man-in-the-middle

Согласно RFC 4251 [4] протокол SSH предлагает 3 способа аутентификации клиентов:

1. Аутентификация с использованием открытых ключей.

При использовании этого способа аутентификации предполагается, что клиентский хост не компрометирован. Также предполагается, что закрытый ключ сервера не компрометирован. В целях ослабления риска для закрытых ключей можно использовать дополнительные пароли (passphrase). Сервер может требовать одновременно пароль и открытый ключ, однако это требование ведет к тому, что пользовательский пароль становится известным серверу

2. Парольная аутентификация.

Парольный механизм, как задано протоколом аутентификации, предполагает, что сервер не компрометирован. При компрометации сервера использование парольной аутентификации будет раскрывать атакующему комбинации имен пользователей и паролей, что может вести к дальнейшему возрастанию риска.

Эту уязвимость можно преодолеть за счет использования другой формы аутентификации. Например, аутентификация на основе открытых ключей не делает допущений об уровне безопасности сервера.

3. Аутентификация по хостам.

Аутентификация по хостам предполагает, что клиентские хосты не компрометированы. Для этого варианта не существует стратегий снижения риска кроме использования аутентификации по хостам в комбинации с другими методами аутентификации.

**2. Настройка маршрутизатора Cisco для подключения по SSH.** Существуют две версии протокола SSH: SSH-1 и SSH-2. В первой версии протокола есть существенные недостатки, поэтому в настоящее время SSH-1 практически нигде не применяется [7]. (Документ RFC 4251 описывает архитектуру SSH-2).

Маршрутизаторы Cisco работают под управлением межсетевой операционной системы (Interwork Operating System – IOS) [8]. Протокол SSH версии 2 был внедрен в некоторые платформы и образы IOS, начиная с Cisco IOS 12.1(19)E [9].

Процесс настройки маршрутизатора можно разделить на несколько этапов.

На первом этапе следует изменить конфигурацию так, чтобы при подключении по линиям vty (виртуальные терминальные линии маршрутизатора) нужно было вводить имя пользователя и пароль, настроенные локально:

Router > **enable**

Router # **configure terminal**

Router (config) # **line vty 0 15**

Router (config-line) # **login local**

На втором этапе необходимо указать маршрутизатору, что он должен принимать сеансы SSH, а также настроить вторую версию протокола:

Router (config-line) # **transport input ssh**

Router (config-line) # **exit**

Router (config-line) # **ip ssh version 2**

Следующий этап – необходимо настроить несколько пар имен и паролей в режиме глобальной конфигурации маршрутизатора:

Router (config) # **username user password pass**

На четвертом этапе нужно указать имя устройства, доменное имя устройства и пароль для привилегированного режима:

Router (config) # **hostname R1**

R1 (config) # **ip domain-name example.com**

R1(config) # **enable secret strongpassword**

На последнем этапе необходимо использовать команду, создающую ключи rsa:

R1 (config) # **crypto key generate rsa**

Каждому клиенту SSH потребуется копия открытого ключа, чтобы установить соединение, поэтому клиент автоматически запрашивает ключ у устройства, загружает его в начале сеанса и в большинстве программ переспрашивает в диалоговом окне у пользователя, принимать ключ или нет [8].

**3. Подключение и анализ трафика.** Для тестирования подключения к маршрутизатору по протоколу SSH построим простейшую сеть, изображенную на рис. 2, которая состоит из хоста и маршрутизатора.

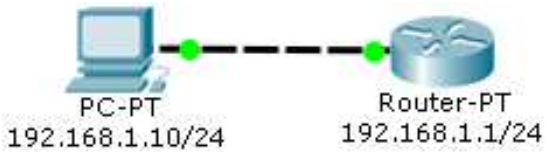


Рис. 2. Используемая сеть

Хост имеет IP-адрес 192.168.1.10 и маску подсети 255.255.255.0. Интерфейс маршрутизатора, подключенный к хосту, имеет IP-адрес 192.168.1.1 и маску подсети 255.255.255.0.

Для подключения к серверу SSH существует несколько свободно распространяемых программ-клиентов SSH, например, PuTTy, TeraTerm и другие. При подключении с помощью одной из программ необходимо выбрать используемый протокол (SSH-2), ввести IP-адрес маршрутизатора (192.168.1.1), затем ввести логин и пароль, которые были настроены в пункте 2 статьи (user, pass). При успешном подключении появится консоль маршрутизатора, с помощью которой можно производить настройку.

Мониторинг и анализ сетевого трафика являются неотъемлемой частью процесса управления компьютерной сетью, используются для диагностики, тестирования и поиска неисправностей в сети, для выявления проблем в обеспечении безопасности компьютерной сети

и информации, циркулирующей в ней [10]. Используем программу-анализатор трафика, например Wireshark. При включенном захвате трафика укажем в консоли маршрутизатора несколько настроек, например, пароль для консольного подключения, как показано на рис. 3.

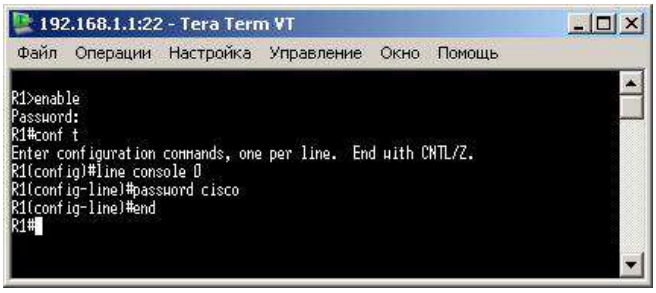


Рис. 3. Настройка пароля для консольного подключения

В окне программы Wireshark видно, что данные через сеть передаются в зашифрованном виде (рис. 4).

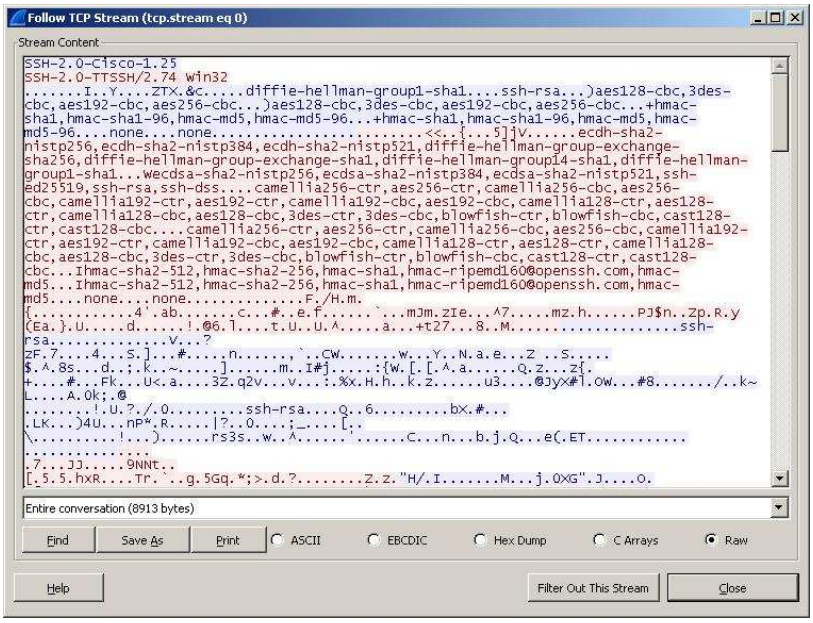


Рис. 4. Захваченные данные

**Выводы.** Как известно, невозможно достичь стопроцентной безопасности. Но можно существенно уменьшить вероятность реализации угроз безопасности, рационально используя различные средства и методы защиты.

Использование протокола SSH для управления оборудованием рекомендовано компанией Cisco [11].

Современное сетевое оборудование имеет достаточно много других функций для обеспечения защиты, например, привязка MAC-адресов к портам, создание виртуальных локальных сетей (VLAN), защита от DoS атак и т.д.

С помощью руководства [11] в дальнейшем будут изучены другие функции защиты, которые содержит сетевое оборудование Cisco, а так же настройка эффективность этих функций.

**Библиографический список**

1. Олифер В.Г., Олифер Н.А. Компьютерные сети: Принципы, технологии, протоколы. – 3-е изд. – СПб.: Питер, 2006. – 958 с.

2. Анатольев А.Г. Дистанционное управление компьютером. Терминалы и протоколы удаленного управления [Электронный ресурс] (Учебно-метод. материалы для студ. кафедры АСОИУ ОмГТУ). – URL: http://www.4stud.info/networking/lecture8.html (дата обращения: 08.04.2016).

3. Курбатов Д. Популярное сетевое оборудование и статистика уязвимостей [Электронный ресурс]. – 2012. – 20 апреля. – URL: https://habrahabr.ru/company/pt/blog/142479 (дата обращения: 17.04.2016).

4. RFC 4251. The Secure Shell (SSH) Protocol Architecture [Электронный ресурс]. – URL: https://www.ietf.org/rfc/rfc4251.txt (дата обращения: 12.04.2016).

5. RFC 4251. Архитектура протокола SSH [Электронный ресурс] / пер. с англ. Н. Малых. – URL: http://rfc.com.ru/rfc4251.htm (дата обращения: 12.04.2016).

6. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2015. – 960 с.

7. Лубягин А.В. Краткое введение в SSH [Электронный ресурс]. – 2007. – Сентябрь. – URL: http://pacify.ru/ssh-intro (дата обращения: 16.04.2016).

8. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822: пер. с англ. – 3-е изд. – М.: Вильямс, 2013. – 720 с.

9. Настройка Secure Shell на маршрутизаторах и коммутаторах с программным обеспечением Cisco IOS [Электронный ресурс]. – 2008. –

23 марта. – URL: http://www.cisco.com/cisco/web/support/RU/9/92/92052_ssh.html (дата обращения: 16.04.2016).

10. Защита информации в компьютерных сетях. Практический курс: учеб. пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский [и др.]; под ред. Н.И. Синадского. – Екатеринбург: Изд-во УГТУ-УПИ, 2008. – 248 с.

11. Руководство Cisco по усилению защиты устройств Cisco IOS [Электронный ресурс]. – 2013. – 28 июля. – URL: http://www.cisco.com/cisco/web/support/RU/106/1068/1068484_21.pdf (дата обращения: 16.04.2016).

## References

1. Olifer V.G., Olifer N.A. Komp'iuternye seti: Printsipy, tekhnologii, protokoly [Computer networks: principles, technologies and protocols]. Saint Petersburg: Piter, 2006. 958 p.

2. Anatol'ev A.G. Distantsionnoe upravlenie komp'iuterom. Terminaly i protokoly udalennogo upravleniia [Computer remote control. Terminals and protocols of remote control], available at: http://www.4stud.info/networking/lecture8.html (accessed 08 April 2016).

3. Kurbatov D. Populiarnoe setevoe oborudovanie i statistika uiazvimostei [Popular network equipment and statistics of the vulnerabilities], 2012, 20 April, available at: https://habrahabr.ru/company/pt/blog/142479 (accessed 17 April 2016).

4. RFC 4251. The Secure Shell (SSH) Protocol Architecture, available at: https://www.ietf.org/rfc/rfc4251.txt (accessed 12 April 2016).

5. RFC 4251. Arkhitektura protokola SSH [The Secure Shell (SSH) Protocol Architecture], available at: http://rfc.com.ru/rfc4251.htm (accessed 12 April 2016).

6. Tanenbaum E., Uezeroll D. Komp'iuternye seti [Computer Networks]. Saint Petersburg: Piter, 2015. 960 p.

7. Lubiagin A.V. Kratkoe vvedenie v SSH [Brief introduction to SSH], 2007, September, available at: http://pacify.ru/ssh-intro (accessed 16 April 2016).

8. Odom U. Ofitsial'noe rukovodstvo Cisco po podgotovke k sertifikatsionnym ekzamenam CCENT/CCNA ICND1 640-822 [Official guide of Cisco to preparation for certified examinations CCENT/CCNA ICND1 640-822]. Moscow: Vil'iams, 2013. 720 p.

9. Nastroika Secure Shell na marshrutizatorakh i kommutatorakh s programmnym obespecheniem Cisco IOS [Configuration Secure Shell on Routers and Switches Running Cisco IOS], 2008, 23 March, available at: http://www.cisco.com/cisco/web/support/RU/9/92/ 92052_ssh.html (accessed 16 April 2016).

10. Andronchik A.N., Bogdanov V.V., Domukhovskii N.A. [et al.]. Zashchita informatsii v komp'iuternykh setiakh. Prakticheskii kurs [Information security in computer networks. Practical course]. Ekaterinburg: Ural'skii gosudarstvennyi tekhnicheskii universitet – UPI imeni pervogo Prezidenta Rossii B.N. El'tsina, 2008. 248 p.

11. Rukovodstvo Cisco po usileniiu zashchity ustroistv Cisco IOS [Guide of Cisco to strengthening of protection of Cisco IOS devices], 2013, 28 July, available at: http://www.cisco.com/cisco/web/support/RU/106/ 1068/1068484_21.pdf (accessed 16 April 2016).

## Сведения об авторах

**Бортник Дмитрий Аркадьевич** (Пермь, Россия) – студент Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр-т, 29, e-mail: bortnikdmitriy@mail.ru).

**Кротова Елена Львовна** (Пермь, Россия) – кандидат физико-математических наук, доцент кафедры высшей математики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр-т, 29, e-mail: lenkakrotova@yandex.ru).

## About the authors

**Bortnik Dmitry Arkadyevich** (Perm, Russian Federation) is a Student of Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: bortnikdmitriy@mail.ru).

**Krotova Elena Lvovna** (Perm, Russian Federation) is a Ph.D. in Physico-Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: lenkakrotova@yandex.ru).

Получено 20.04.2016