Эссе по курсу "Защита информации"
кафедра радиотехники
Московский физико-технический институт (ГУ МФТИ)

Сафонов Александр
17 марта 2006г

Протокол управления доступом TACACS+ (Access control protocol TACACS+)

http://www.re.mipt.ru/infsec

Содержание

1. Технологии обеспечения безопасности данных

В настоящее время существуют различные технологии, направленные на обеспечение безопасности данных, в котором выделяются 3 важнейших компонента:

1. аутентификация (с последующей авторизацией)
2. сохранение целостности данных (их неизменность и конфиденциальность обеспечивается безопасностью инфраструктуры сети)
3. активная проверка установленной политики безопасности

В данном эссе все внимание обращено на первый компонент – аутентификацию.

2. Технологии аутентификации

Первым и наиболее распространенным до сих пор средством проведения аутентификации было использование паролей. Для обеспечения высокого уровня безопасности пароли необходимо часто менять, а криптографически стойкие пароли неудобны для запоминания пользователями, что в итоге привело к формированию методики использования одноразовых паролей. Среди них: аутентификация по протоколу S/Key или при помощи специальных аппаратных средств: смарт-карт, USB-токенов и т.д. Для модемного доступа наиболее распространен механизм аутентификации по протоколу PPP с использованием протоколов PAP, CHAP и EAP. Протокол EAP продолжают усовершенствовать с целью расширения его функциональности, но в настоящее время он уже позволяет более гибко использовать как существующие, так и будущие технологий аутентификации в каналах PPP. А в среде корпоративного удаленного доступа большое распространение получили протоколы, которые поддерживают масштабируемые решения в области аутентификации - TACACS+ и Remote Access Dial-In User Service (RADIUS).

3. TACACS+

TACACS+ - это протокол третьего поколения в семействе протоколов TACACS (RFC 1492). TACACS (Terminal Access Controller Access Control System) – это протокол удаленной аутентификации, который применяется в процессе предоставления доступа к информационным серверам, серверам удаленного доступа и другим активным сетевым устройствам. Он был разработан U.S. Department of Defense и BBN Planet corp. (Bolt, Beranek and Newman, Inc). В дальнейшем он несколько раз дорабатывался компанией Cisco Systems Inc. В результате сначала появилась улучшенная версия протокола – XTACACS, а спустя некоторое время – полностью новый протокол TACACS+, который не совместим с предыдущими версиями протокола.

В своей работе протоколы семейства TACACS используют порт 49, который выделило для них Internet Assigned Numbers Authority (IANA). Предыдущие версии TACACS (как и аналогичный протокол RADIUS) в качестве средства доставки использовали протокол UDP. В отличие от них, TACACS+ полагается на TCP, что позволяет за счет несколько больших накладных расходов обеспечить более простую реализацию и расширить функциональность (например, поддерживается множественная обработка запросов).

TACACS+ - это протокол, реализованный по технологии клиент-сервер, причем почти всегда клиент – это NAS (Network Access Server - сервер сетевого доступа; например, Cisco AS5300 и Shiva Corp.'s Access Manager 3.0), а сервер – некоторая программа, запущенная на хост-машине (UNIX, NT или другая, необходимо отметить что UNIX системы наиболее распространены в роли серверов TACACS+). Примером таких серверов являются CiscoSecure Access Control Server (ACS) и Shiva's LAN Rover/E Plus.
Протокол TACACS+ позволяет объединить несколько NAS в общую систему обеспечения аутентификации в рамках системы обеспечения сетевой безопасности, функционируя в 2 режимах:

1. проведение аутентификации, используя централизованную базу учетных записей,
2. посредничество для внешних систем аутентификации (т.н. proxy-режим).

Благодаря этому он может использоваться и в глобальных системах предоставления безопасного сетевого доступа, таких как CiscoSecure Global Roaming Server (GRS).

Принципиально важной особенностью протокола TACACS+ является то, что он позволяет разделить аутентификацию, авторизацию и учет (AAA — Authentication,

Authorization, Accounting) и реализовать их на отдельных серверах. Это является существенным прогрессом по сравнению как с исходным протоколом TACACS, в который понятие учета вообще не входило, так и с протоколом RADIUS, в котором аутентификация и авторизация совмещены. Далее мы рассмотрим аутентификацию, авторизацию и учет более подробно.

TACACS+ может передавать различные виды аутентификационной информации. Он поддерживает множество механизмов аутентификации - PAP, CHAP, Kerberos 5 и многие другие. Протокол является расширяемым, что позволяет добавлять новые механизмы, такие как KCHAP. Также поддерживаются многоэтапные challenge-response сессии, что предоставляет дополнительные возможности при работе с аутентификацией с применением специальных аппаратных средств - токенов. В то же время, аутентификация не является обязательной (она может применяться для ограниченного набора сервисов или не применяться вовсе), что является еще одним свидетельством чрезвычайной гибкости протокола.

TACACS+ обеспечивает механизм передачи серверу сетевого доступа информации об access list'е ("списке разрешенных действий") подключенного пользователя. Таким образом реализуется авторизация — процесс определения действий, которые позволены данному пользователю. Аутентифицирование не является обязательным условием для авторизации (но тогда в запросе на авторизацию следует указать, что аутентификация пользователя не проведена). В любом случае доступ к запрашиваемым сервисам зависит только от примененной политики в области безопасности (фактически, от access list'ов). Хотя протокол TACACS+ допускает только "успешную" или "не успешную" авторизацию, возможна дополнительная настройка. Еще раз доказывает чрезвычайную гибкость протокола то, что возможна отдельная авторизация для каждого сервиса при единственной аутентификации.

TACACS+ передает учетную информацию для биллинг-сервера с помощью TCP, гарантируя достоверность и наибольшую возможную полноту отчета о действиях пользователя. С помощью учетной функции обычно решаются 2 задачи:

1. Тарификация на основе информации о том, какими сервисами воспользовался пользователь.
2. Обнаружение вторжений на основе информации о действиях пользователя

TACACS+ в момент своего появления поддерживал (как и его предшественник XTACACS) только 2 типа учетных записей: "start" – начато использование сервиса, "stop"

– закончено использование. В процессе доработки протокола появился третий тип учетных записей – “update”. TACACS+ раз в X секунд сообщает биллинг-серверу о том, что сервис предоставляется, а также обновляет информацию об общем времени использования сервиса. Эти данные могут быть весьма полезны, например, ISP (internet service provider) для верной тарификации. Учетная запись может содержать следующую информацию: имя пользователя, используемый (запрашиваемый) сервис, используемый протокол, дату, время начала и окончания соединения, порты, адреса, число переданных пакетов и байт, выполненные команды (для exec и Telnet сессий). Следует отметить, что формат этих записей строго не задан и может изменяться при необходимости.

Рассмотрим теперь вопрос безопасности протокола. Первое, сервер должен доверять клиенту. Для гарантирования этого используются как таблицы IP-адресов (и, возможно, других данных) известных клиентов, так и т.н. “разделяемый секрет” – последовательность символов, которая используется в шифровании пакетов и никогда не передается по каким-либо каналам связи. Он устанавливается администратором вручную и на сервере, и на клиенте. По умолчанию TACACS+ шифрует весь трафик между сервером и клиентом. Тело пакета в этом случае шифруется целиком, а остаются лишь стандартные TACACS+ заголовки (см. Приложение), не несущие ценной информации. В них есть поле, именно в котором и указано – шифруется ли “тело” пакета. Для отладки возможно использование режима без шифрования. Для сравнения, в протоколе Radius шифруется только пароль в “access-request” пакете, а все остальная информация передается открыто. Следовательно, такие данные, как имя пользователя, авторизованные сервисы или учетная информация, могут быть захвачены посторонними лицами, что составляет серьезнейшую угрозу безопасности.

Перейдем теперь к более детальному рассмотрению процесса взаимодействия пользователь-клиент-сервер, которое показано на нижеприведенном рисунке.

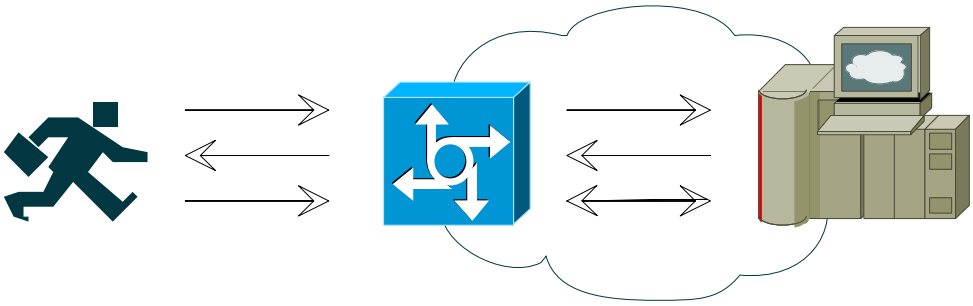

Рисунок 1: Взаимодействие между пользователем и системой TACACS+ [1]

1. Пользователь инициирует соединение с клиентом TACACS+	5. Сервер TACACS+ сообщает результаты идентификации
2. Клиент TACACS+ запрашивает у пользователя имя и пароль	6. Клиент и сервер обмениваются авторизовационной информацией
3. Пользователь отвечает на запрос	7. Клиент TACACS+ обрабатывает параметры, полученные во время авторизации
4. Клиент TACACS+ посылает зашифрованный пакет серверу TACACS+	

1

2

3

А теперь обратим внимание на взаимодействие между клиентом и сервером TACACS+ (за что в первую очередь и отвечает этот протокол):

1. Клиент отправляет серверу сообщение “START”, которое всегда включает в себя тип аутентификации и может включать имя пользователя, а также дополнительные аутентификационные данные.
2. В ответ сервер отправляет сообщение “REPLY”, содержащее информацию о том, завершена ли аутентификация или для этого требуются дополнительные данные.
3. Если аутентификация еще не завершена, клиент посылает серверу сообщение “CONTINUE” , содержащее запрошенную информацию. Обмен сообщениями “CONTINUE”-“REPLY” продолжается пока на сервере TACACS+ не будет проведена.аутентификация пользователя, подключенного к клиенту.
4. Далее может быть начат процесс авторизации. Клиент отправляет серверу сообщение “REQUEST”. Оно содержит обязательные поля, содержащие информацию о пользователе (например, его имя), а также набор опциональных полей, детально описывающих запрошенные сервисы.

4. Заключение

В заключение хотелось бы отметить тот факт, что в настоящее время разработан новый протокол Diameter (RFC 3588 (Diameter Base Protocol), RFC 3589 (Diameter Command Codes for 3GPP), RFC 4006 (Diameter Credit-Control Application)) – наследник RADIUS, который включил большую часть функциональности TACACS+. Но в то же время компания Cisco Systems продолжит поддерживать свой протокол TACACS+, который остается непревзойденным для управления предоставлением доступа к сетевым устройствам (а не к сети через PPP,VPN), т.к. он единственный поддерживает такие дополнительные возможности, как фильтрация команд. Детальное сопоставление с протоколом Diameter можно будет произвести, когда он станет более распространен и поддержан производителями решений в AAA-области.

5. Приложение

Формат кадра

4	8	16	24	32 bit
Major	Minor	Packet Type	Sequence #	Flags
Session ID				
Length				

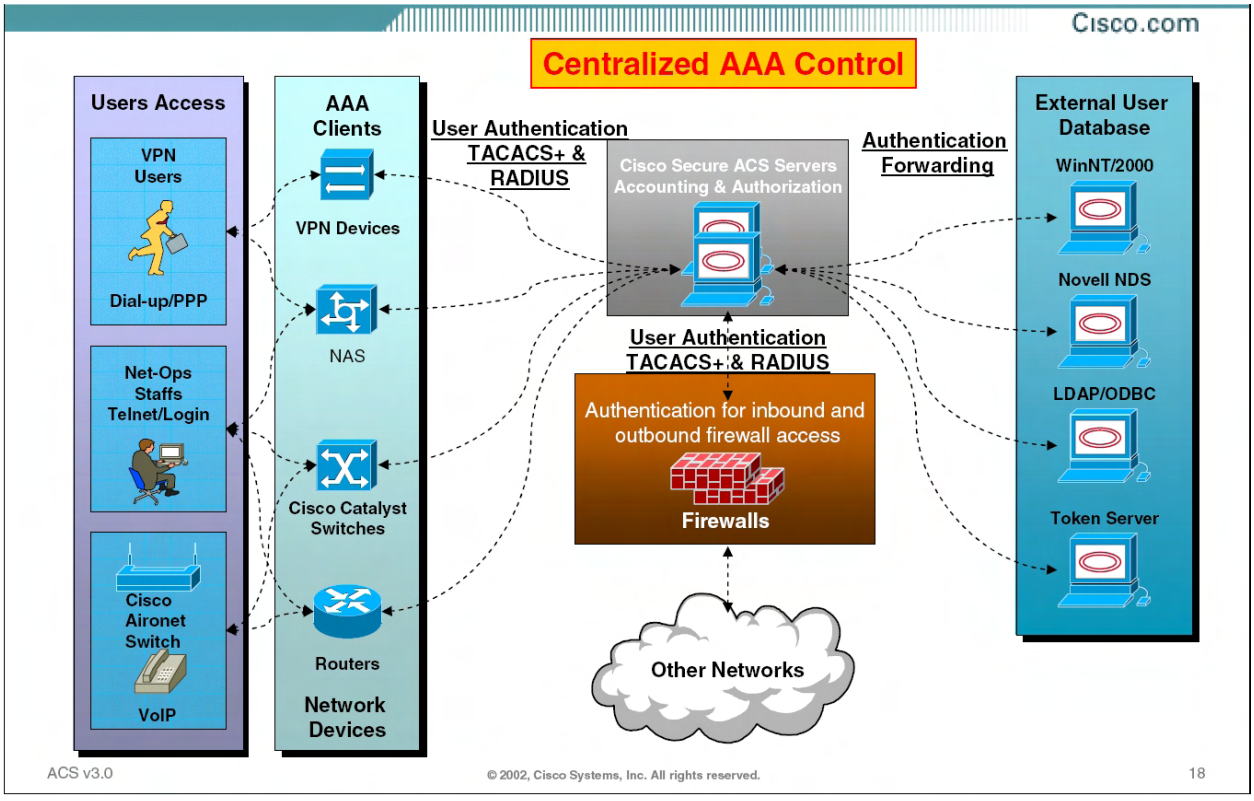

Рисунок 2: Схема централизованного AAA решения [6]

6. Ссылки по теме

1. Описание технологии аутентификации TACACS+, Cisco System Inc., 2003 http://www.cisco.com/russian_win/warp/public/3/ru/solutions/sec/mer_tech_ident-tacacs.html
2. Технологии идентификации - Обеспечение безопасности в сети, Cisco Systems Inc. www.cisco.com/global/RU/win/solutions/sec/mer_tech_ident.shtml
3. Single-User Network Access Security TACACS+, Cisco System Inc., Mar 30, 1995 http://www.cisco.com/warp/public/614/7.html
4. RFC #1492: An Access Control Protocol, Sometimes Called TACACS, *C.Finseth*, University of Minnesota, 1993 http://tools.ietf.org/html/1492
5. CiscoSecure Access Control Server: Primer Introduction, Cisco System Inc., 2005 http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c1161/cdccont_0900aecd8040daa7.pdf
6. CiscoSecure Access Control Server: Tutorial, Cisco System Inc., 2002 http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c1161/ccmigration_09186a0080159f3f.pdf
7. Authentication Protocols: TACACS+ & RADIUS comparison, Cisco System Inc., Jan 19, 2006 http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml
8. Guarding The Flank With RADIUS & TACACS+, *Dan Backman, 2001* http://www.networkcomputing.com/902/902ws1.html
9. Протоколы RADIUS и TACACS+: сравнение и принципы функционирования, *Владислав Пинженин*, *Максим Мокроусов*, Сетевые решения, 2003 http://www.opennet.ru/base/cisco/radius_tacacs.txt.html
10. Introduction to Diameter: Get the next generation AAA protocol, *Jeffrey Liu*, *Steven Jiang*, *Hicks Lin*, IBM, Jan 24, 2006 http://www-128.ibm.com/developerworks/library/wi-diameter/?ca=dnw-703