A. Bakshaev
Category: Information Security
May 2005
http://www.re.mipt.ru/infsec

Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ)
http://www.re.mipt.ru/infsec

Протокол Radius управления сетевым доступом и поддержка EAP (Extensible Authentication Protocol) в нем.

Abstract

В этой статье обзорно описывается протокол сетевой аутентификации **Radius** (RFC2865) и реализация поддержки в данном протоколе **EAP** (Extensible Authentication Protocol), протокола, поддерживающего самые разные способы аутентификации. В рассматриваемой схеме Network Access Server (**NAS**) обменивается EAP – пакетами с Radius – сервером (EAP – поля инкапсулированы в пакетах Radius). Преимуществом этого является полная свобода в выборе методе аутентификации EAP, т.к. на стороне **NAS** (маршрутизатор Cisco, например) не требуется какой-либо специфической реализации метода, все функции EAP – аутентификатора осуществляет Radius – сервер. На данный момент поддержка Radius и Tacacs реализована в IOS – ах практически всех современных маршрутизаторов, что позволяет с легкостью поддерживать EAP - аутентификацию PPP или IEEE 802 – клиентов. При этом EAP предполагает использование самых различных конечных реализаций аутентификации, в том числе смарт-карт, системы Kerberos [RFC1510], аутентификации с помощью открытого ключа и т.п.

В эссе употребляются следующие определения и понятия:

Remote Authentication Dial In User Service (RADIUS) – метод аутентификации, авторизации и аккаунтинга сетевого доступа.

Extensible Authentication Protocol (EAP) – аутентификационная платформа, на базе которой возможна реализация различных аутентификационных механизмов. EAP может использоваться для аутентификации в сетях самых разных масштабов, в том числе и беспроводных.

Peer – проходящий аутентификацию клиент (PPP или 802.1X, например)

Authenticator – непосредственно, само устройство (**Network Access Server (NAS)** или **RADIUS client**), предоставляющее доступ или отказывающее в нем, осуществляя форвардинг EAP – пакетов от Peer – а на производящий аутентификацию **Authentication server.**

Authentication server – машина, непосредственно реализующая поддержку Radius и EAP.

При этом в случае успешной аутентификации, осуществляется **авторизация**, в результате которой NAS принимает решение о предоставлении Peer – у того или иного сервиса.

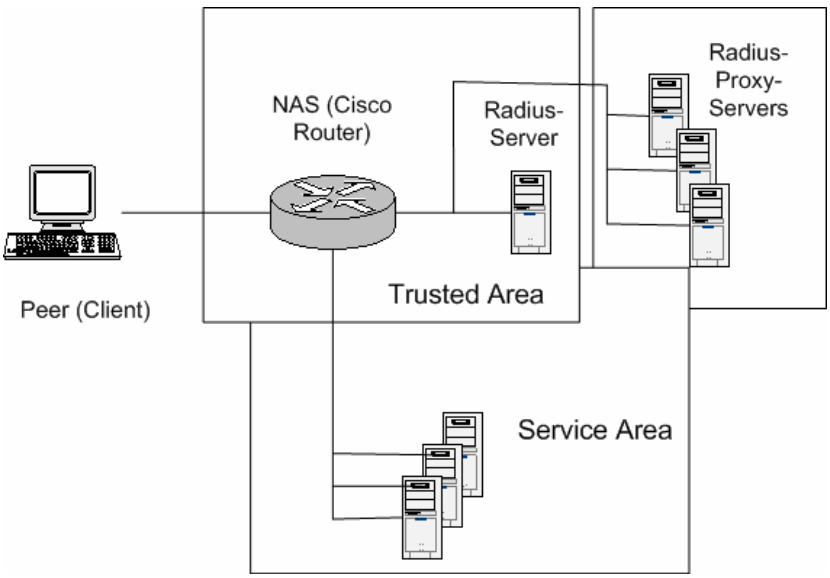
Service – сервис, для доступа к которому клиент осуществляет аутентификацию.

В случае успешной авторизации между клиентом и машиной, предоставляющей сервис, устанавливается сеанс.

Session – сеанс связи между NAS и Peer-ом, статистика которого полностью ведется NAS – машиной. При необходимости эта статистика может предоставляется NAS – ом Radius – серверу, для этого в протоколе Radius существует множество атрибутов. Процесс сбора статистики по установленной сессии (время инициализации и завершения, и т.п.) называется
аккаунтингом.

Accounting - аккаунтиг.

Процесс аутентификации



В схеме Radius/EAP Radius является “промежуточным” протоколом для переноса EAP – сообщений между NAS и Radius – сервером. При этом на уровне клиент NAS аутентификация осуществляется на уровне EAP. Рассмотрим общую схему аутентификации. После начального обмена пакетами между клиентом и NAS, подразумевающего объявление EAP в качестве протокола аутентификации, NAS-сервер посылает клиенту EAP-Request/Identity. Клиент посылает EAP-Response, в котором содержатся его идентификационные данные. Далее NAS инкапсулирует EAP-Response в EAP-Message контейнер Access-Request пакета Radius, причем EAP – пакет инкапсулируется целиком. В случае получения правильного Access-Request пакета Radius-server формирует Access-Challenge пакет с тем или иным типом EAP-Request в качестве EAP-Message. Если Radius-server не поддерживает EAP, то NAS получает Access-Reject пакет, и клиент не допускается к авторизации. Повторная сессия аутентификации возможна только по истечении определенного таймаута. Тип EAP-Request будет зависеть от типа EAP аутентификации, предусмотренного клиентом и аутентификатором [5]:

1. **Nak (Response only)**
2. **MD5-Challenge**
3. **One-Time Password (OTP) (RFC 1938)**
4. **Generic Token Card**
5. **EAP Cisco Wireless (LEAP)**
6. **EAP-TLS**

Информацию по данным типам аутентификации можно найти в соответствующих RFC

Далее NAS декапсулирует EAP-Challenge и доставляет пакет клиенту. Здесь нужно отметить, что EAP – пошаговый протокол, невыполнение условий какого-либо шага должно вести к получению NAS-ом Access-Reject – пакета. Такая пересылка EAP-пакетов продолжается, пока NAS не получит Access-Accept или Access-Reject пакет от Radius-сервера, и клиенту будет предоставлен необходимый сервис, или ему будет отказано в доступе. Это осуществляется пакетами Access-Accept с атрибутом EAP Success в контейнере EAP-Message или Access-Reject с EAP Failure в EAP-Message соответственно.

В случае превышения таймаута получения EAP – пакета от клиента, аутентификационная сессия прерывается.

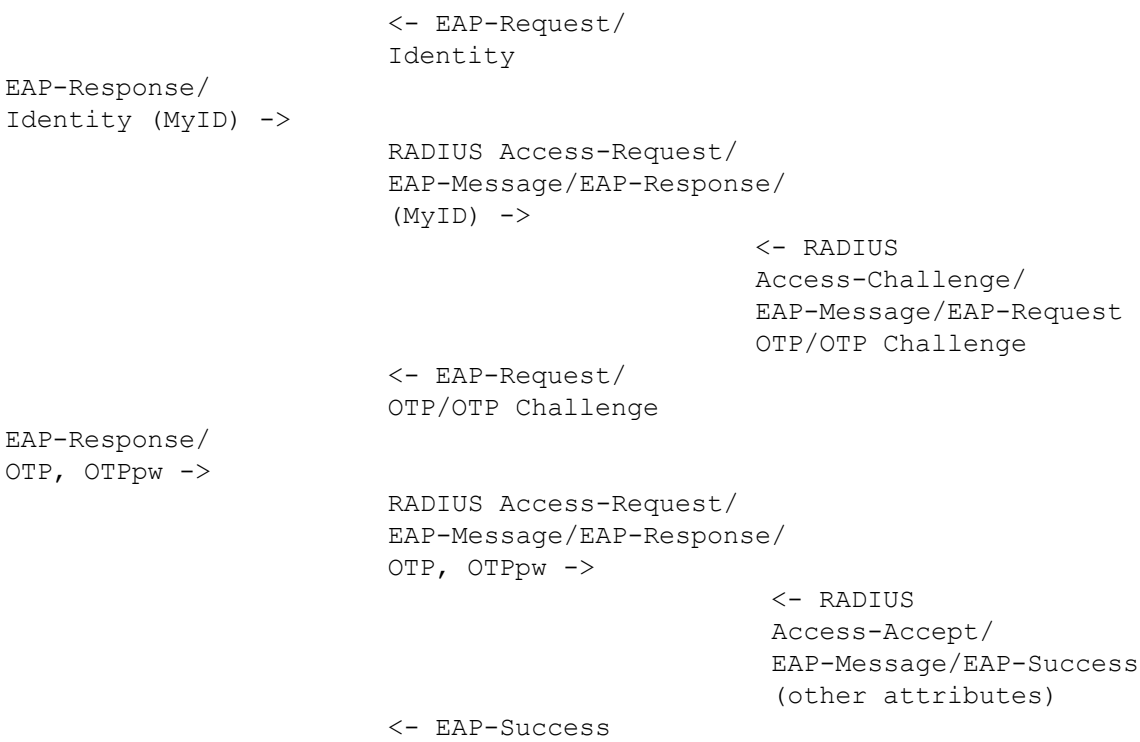
NAS копирует Type-Data поле EAP-Response/Identity-пакета, полученного от клиента, в атрибут User-Name пакета Radius, что необходимо для Radius-проксирования. Начальный EAP-запрос обычно осуществляется NAS-ом, это позволяет аутентифицировать некоторых клиентов локально, а также уменьшить загрузку Radius-сервера. Защита NAS сервера от Denial of Service (DoS) атак осуществляется уменьшением размера буфера и ограничением числа неправильных EAP-пакетов.

EAP-Message

Как уже говорилось, EAP-Message представляет собой контейнер пакета Radius, в который NAS инкапсулирует EAP – пакеты, пришедшие от Peer-а. В связи с тем, что EAP поддерживает множество криптостойких методов аутентификации, необходимо обеспечить защиту RADIUS/EAP от атак (например, изменения содержимого Radius/EAP Success или Radius/EAP Failure пакетов), необходима криптозащита на уровне отдельного Radius – пакета, а также проверка целостности пакета. Для защиты Access-Request, Access-Challenge, Access-Accept, и Access-Reject пакетов, находящихся в контейнере EAP-Message используется так называемый **Message-Authenticator**. Пакеты Access-Request, с EAP-Message, не имеющие соответствующего Message-Authenticator-а, или Message-Authenticator которых не совпадает с рассчитанным Radius-Server-ом, игнорируются. Message-Authenticator представляет собой HMAC-MD5 хэш всего Access-Request пакета, включая ID, Length и Ahenticator, используя
shared secret в качестве ключа

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes)

В соответствующем **RFC3579** описаны возможные варианты EAP – аутентификации Peer – а.
Рассмотрим один из них, в котором рассматривается использование OTP (**A One-Time Password** System) в качестве типа Request/Response для EAP:



После установления соединения аутентификация клиента начинается с EAP запроса NAS с целью идентификации клиента. Возвращенный MyID NAS перенаправляет аутентификатору (Radius – серверу) в Radius – пакете, причем EAP атрибуты (Message: Request, Response, Success, Failure), соответствующие кодовому (Code) полю пакета EAP, теперь инкапсулируются в EAP-Message поле Access-Request пакета Radius. Еще раз нужно отметить, что на уровне Peer- NAS обмен данными осуществляется на уровне пакетов EAP (поля EAP инкапсулированы в фрейме пакета PPP, TCP - сессия). На уровне NAS - Authentication server (RADIUS) используются UDP Radius пакеты, при этом сегмент сети, объединяющий NAS и Radius-server мы принимаем как **reliable** и считаем этот сегмент зоной пониженной опасности. Далее NAS перенаправляет EAP/OTP – запрос от Radius – сервера к клиенту и возвращает от клиента в качестве OTPpw, как правило *, 64-bit MD-5 – пароль *.

Аутентификатор же, в свою очередь, возвращает NAS-серверу Access-Accept или Access-Reject с соответствующим значением EAP-Message. Результатом является предоставление клиенту сервиса с началом аккаунтинга или отказ от дальнейшей работы с данным клиентом на определенное время.

* Возможными идентификаторами применяющегося в OTP алгоритма по [4] являются

md4	MD4 Message Digest
md5	MD5 Message Digest
sha1	NIST Secure Hash Algorithm Revision 1

При этом при EAP- аутентификации клиентская сторона получает специальные параметры для локального OTP – генератора от Radius-server (они являются частью OTP-запроса)

Ссылки на использованные в статье материалы:

1) **rfc2138** Remote Authentication Dial In User Service (RADIUS)
http://www.ietf.org/rfc/rfc2138.txt?number=2138

2) **rfc2139** RADIUS Accounting
http://www.ietf.org/rfc/rfc2139.txt?number=2139

3) **rfc3579** RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
http://www.ietf.org/rfc/rfc3579.txt?number=3579

4) **rfc1938** A One-Time Password System
http://www.ietf.org/rfc/rfc1938.txt?number=1938

5) **rfc2284** PPP Extensible Authentication Protocol (EAP)
http://www.ietf.org/rfc/rfc2284.txt?number=2284

Непосредственный владелец **RFC**:
The Internet Engineering Task Force http://www.ietf.org