دليل أستكشاف أخطاء مصادق RADIUS ومصدق الرسائل وإصلاحها غير صالح

المحتويات

المقدمة

يصف هذا المستند آليتي أمان RADIUS:

- رأس المصدق
- سمة مصدق الرسائل

تغطي هذه الوثيقة ما هي آليات الأمان، وكيف يتم إستخدامها، ومتى يجب أن تتوقع فشل التحقق من الصحة.

رأس المصدق

وفقا لمعيار RFC 2865، يبلغ طول رأس المصدق 16 بايت. وعند إستخدامه في طلب الوصول، يسمى مصدق الطلب. عند إستخدامه في أي نوع من الاستجابة، يطلق عليه مصدق الاستجابة. تستخدم من أجل:

- مصادقة الاستجابة
- إخفاء كلمة المرور

مصادقة الاستجابة

إذا استجاب الخادم باستخدام "مصدق الاستجابة" الصحيح، يمكن للعميل إجراء الحساب إذا كانت الاستجابة مرتبطة بطلب صالح.

يرسل العميل الطلب مع رأس المصدق العشوائي. بعد ذلك، يقوم الخادم الذي يرسل الاستجابة بحساب مصدق

الاستجابة باستخدام حزمة الطلب مع السر المشترك:

```
(ResponseAuth = MD5(Code + ID + Length + RequestAuth + Attributes + Secret
```

يقوم العميل الذي يستقبل الاستجابة بتنفيذ العملية نفسها. إذا كانت النتيجة هي نفسها، فإن الحزمة صحيحة.

ملاحظة: لا يمكن للمهاجم الذي يعرف القيمة السرية انتحال الاستجابة ما لم يكن قادرا على التعرف على الطلب.

متى ينبغي توقع فشل التحقق من الصحة؟

يحدث فشل التحقق من الصحة إذا لم يعد المحول يقوم بتخزين الطلب مؤقتا (على سبيل المثال، بسبب المهلة). قد تواجه أيضا هذا الأمر عندما يكون السر المشترك غير صالح (نعم - يتضمن Access-Reject أيضا هذا الرأس). بهذه الطريقة، يمكن لجهاز الوصول إلى الشبكة (NAD) اكتشاف عدم تطابق السر المشترك. عادة ما يتم الإبلاغ عنه بواسطة خوادم/عملاء المصادقة والتفويض والمحاسبة (AAA) كعدم تطابق مشترك للمفتاح، ولكنه لا يكشف التفاصيل.

إخفاء كلمة المرور

كما يتم إستخدام رأس المصدق لتجنب إرسال سمة كلمة مرور المستخدم في نص عادي. أولا، يتم حساب ملخص الرسالة 5 (MD5 - سري، المصدق). ثم يتم تنفيذ العديد من عمليات XOR بأجزاء كلمة المرور. تعد هذه الطريقة عرضة للهجمات غير المتصلة (جداول قوس قزح) نظرا لأنه لم يعد ينظر إلى MD5 على أنه خوارزمية قوية أحادية الإتجاه.

هنا ال بايثون نص أن يحسب المستعمل كلمة:

```
:(def Encrypt_Pass(password, authenticator, secret
                                        ()m = md5
                                (m.update(secret+authenticator
return "".join(chr(ord(x) ^ ord(y)) for x, y in zip(password.ljust
                                    (([m.digest()[:16 ,[16:]('0\',16)
```

عمليات إعادة الإرسال

إذا تم تغيير أي من السمات في طلب وصول RADIUS (مثل معرف RADIUS واسم المستخدم وما إلى ذلك)، فيجب إنشاء حقل المصدق الجديد ويجب إعادة حساب كافة الحقول الأخرى التي تعتمد عليه. إذا كان هذا إعادة إرسال، لا ينبغي أن يتغير شيء.

محاسبة

يختلف معنى رأس المصدق بالنسبة إلى طلب الوصول وطلب المحاسبة.

بالنسبة لطلب الوصول، يتم إنشاء المصدق بشكل عشوائي ومن المتوقع أن يتلقى إستجابة تم حساب ResponseAuthenticator عليها بشكل صحيح، مما يثبت أن الاستجابة كانت مرتبطة بذلك الطلب المحدد.

بالنسبة لطلب المحاسبة، فإن المصدق ليس عشوائيا، ولكنه يتم حسابه (وفقا ل RFC 2866):

```
(RequestAuth = MD5(Code + ID + Length + 16 zero octets + Attributes + Secret
```

بهذه الطريقة، يمكن للخادم التحقق من رسالة المحاسبة فورا وإفلات الحزمة إذا لم تتطابق قيمة إعادة الحساب مع قيمة المصدق. ترجع Identity Services Engine (ISE):

```
RADIUS Accounting-Request header contains invalid Authenticator field 11038
```

السبب النموذجي لهذا هو المفتاح السري المشترك غير الصحيح.

سمة مصدق الرسائل

سمة مصدق الرسائل هي سمة RADIUS المحددة في RFC 3579. تستخدم لغرض مشابه: التوقيع والتصديق. ولكن هذه المرة، لا يتم إستخدامها للتحقق من صحة إستجابة ما بل الطلب.

يقوم العميل الذي يرسل طلب الوصول (يمكن أيضا أن يكون خادما يستجيب باستخدام اعتراض الوصول) بحساب رمز مصادقة الرسائل المستندة إلى التجزئة (HMAC-(MD5 من الحزمة الخاصة به، ثم يضيف سمة مصدق الرسائل كتوقيع. وبعد ذلك، يمكن للخادم التحقق من تنفيذه لنفس العملية.

تبدو الصيغة مماثلة لرأس المصدق:

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

تأخذ الدالة HMAC-MD5 في وسيطتين:

- حمولة الحزمة، والتي تتضمن حقل مصدق الرسائل سعة 16 بايت المملوء بالأصفار
- السر المشترك

متى ينبغي إستخدام مصدق الرسائل؟

يجب إستخدام مصدق الرسائل لكل حزمة، والتي تتضمن رسالة بروتوكول المصادقة المتوسع (RFC 3579) (EAP). ويتضمن ذلك كل من العميل الذي يرسل طلب الوصول والخادم الذي يستجيب مع "تحدي الوصول". يجب أن يقوم الجانب الآخر بإسقاط الحزمة بصمت إذا فشل التحقق من الصحة.

متى ينبغي توقع فشل التحقق من الصحة؟

سيحدث فشل التحقق من الصحة عندما يكون السر المشترك غير صالح. بعد ذلك، لا يمكن لخادم AAA التحقق من صحة الطلب.

يخبر ال ISE:

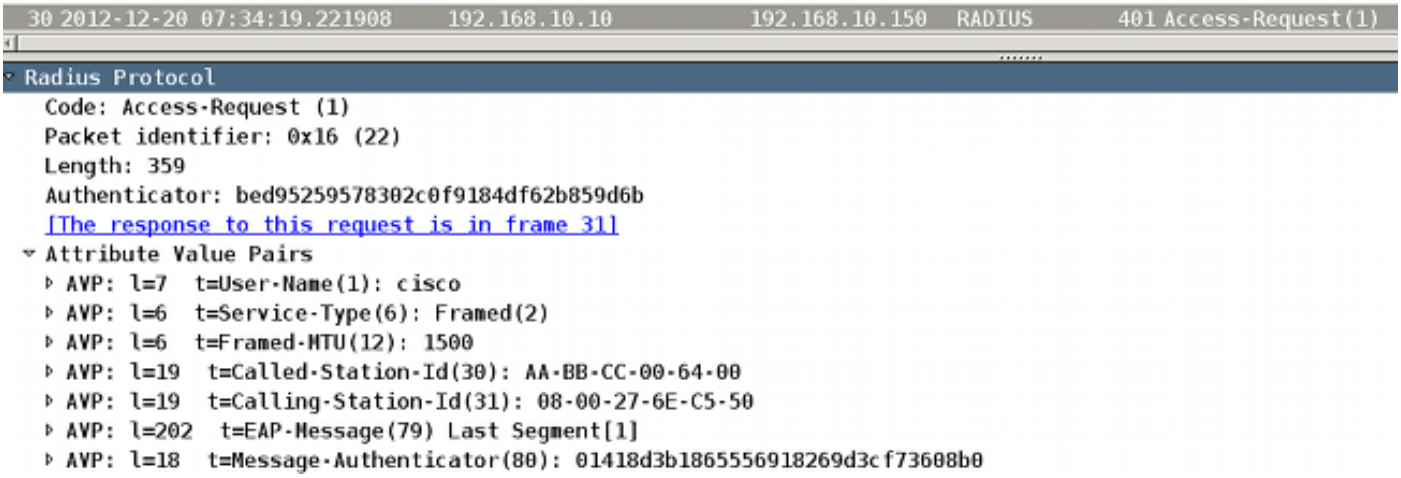
```
.The Message-Authenticator Radius Attribute is invalid 11036
```

ويحدث ذلك عادة في المرحلة اللاحقة عند إرفاق رسالة EAP. لا تتضمن حزمة RADIUS الأولى لجلسة عمل 802.1x رسالة EAP؛ لا يوجد حقل مصدق رسالة ولا يمكن التحقق من الطلب، ولكن في تلك المرحلة، يمكن للعميل التحقق من الاستجابة باستخدام حقل المصدق.

التحقق من صحة سمة مصدق الرسائل

هنا مثال لتوضيح كيفية حساب القيمة يدويا للتأكد من حسابها بشكل صحيح.

تم إختيار الحزمة رقم 30 (طلب الوصول). هو في منتصف جلسة EAP، وتتضمن الحزمة حقل مصدق الرسالة. الهدف هو التحقق من صحة مصدق الرسالة:



1. انقر بزر الماوس الأيمن فوق **بروتوكول Radius** واختر **تصدير وحدات بايت الحزم المحددة**.

2. اكتب حمولة RADIUS إلى ملف (بيانات ثنائية).

3. لحساب حقل مصدق الرسائل، يجب وضع أصفار هناك وحساب HMAC-MD5.

على سبيل المثال، عند إستخدام المحرر سداسي/ثنائي، مثل VIM، بعد كتابة ":xd!"، والتي يتم تحويلها إلى الوضع سداسي العشري والأصفار 16 بايت بدءا من "5012" (50hex هو 80 في ديسمبر وهو نوع مصدق الرسائل، و 12 هو الحجم الذي يساوي 18 بما في ذلك رأس أزواج قيمة السمة (AVP)):

```
0000000: 0116 0167 bed9 5259 5783 02c0 f918 4df6  ...g..RYW.....M.
0000010: 2b85 9d6b 0107 6369 7363 6f06 0600 0000  +..k..cisco.....
0000020: 020c 0600 0005 dc1e 1341 412d 4242 2d43  .........AA-BB-C
0000030: 432d 3030 2d36 342d 3030 1f13 3038 2d30  C-00-64-00..08-0
0000040: 302d 3237 2d36 452d 4335 2d35 304f ca02  0-27-6E-C5-500..
0000050: 4100 c819 8000 0000 be16 0301 0086 1000  A...............
0000060: 0082 0080 880d 0fe6 8421 562e bcf3 75a7  .........!V...u.
0000070: fbf4 9c20 e114 a19d 1282 96d7 45b8 9c26  ... ........E..&
0000080: 86c5 9935 1b2c ca98 1b60 5e91 1c63 d123  ...5.,...`^..c.#
0000090: f019 1ab6 7e2d 0497 1e02 0768 0ac3 aa84  ....~-.....h....
00000a0: 80d5 cd14 92a9 ae31 e9e2 121e 28e8 5f21  .......1....(._!
00000b0: 5c1a 4e20 013f a55b 7b1d 0eb7 1d17 a565  \.N .?.[{......e
00000c0: 626b 2bb4 f756 da05 b51b 043b 346a c51f  bk+..V.....;4j..
00000d0: 98a7 007e ed55 e24b 1cab ec06 799b aed5  ...~.U.K....y...
00000e0: 72c5 451b 1403 0100 0101 1603 0100 28e2  r.E...........(.
00000f0: d25f 2deb 0f0c baf5 570d d3f6 05df 6534  ._-.....W.....e4
0000100: 48d8 0853 00ae 3230 73a9 afb7 ac87 d834  H..S..20s......4
0000110: f7e9 bb57 8ac1 1750 1200 0000 0000 0000  ...W...P........
0000120: 0000 0000 0000 0000 003d 0600 0000 0f05  .........=......
0000130: 0600 00c3 5057 0d45 7468 6572 6e65 7430  ....PW.Ethernet0
0000140: 2f30 181f 3236 5365 7373 696f 6e49 443d  /0..26SessionID=
0000150: 6163 732f 3134 3531 3136 3739 372f 3132  acs/145116797/12
0000160: 3b04 06c0 a80a 0a                        ;.......
```

بعد هذا التعديل، تصبح الحمولة جاهزة. من الضروري العودة إلى الوضع سداسية عشرية/ثنائية (النوع: "!٪- xd r") وحفظ الملف (":wq").

4. أستخدم OpenSSL لحساب HMAC-MD5:

```
'pluton # cat packet30-clear-msgauth.bin | openssl dgst -md5 -hmac 'cisco
stdin)= 01418d3b1865556918269d3cf73608b0)
```

تأخذ الدالة HMAD-MD5 وسيطتين: الأولى من إدخال قياسي (stdin) هي الرسالة نفسها والثانية هي السر المشترك (cisco في هذا مثال). والنتيجة هي نفس قيمة مصدق الرسائل المرفق بحزمة طلب الوصول RADIUS.

نفس الشيء يمكن حسابه باستخدام برنامج Python النصي:

```
pluton # cat hmac.py
usr/bin/env python/!#

import base64
  import hmac
import hashlib

('f = open('packet30-clear-msgauth.bin', 'rb
:try
()body = f.read
:finally
()f.close

(digest = hmac.new('cisco', body, hashlib.md5
()d=digest.hexdigest
print d

pluton # python hmac.py
01418d3b1865556918269d3cf73608b0
```

يوضح المثال السابق كيفية حساب حقل مصدق الرسائل من طلب الوصول. بالنسبة لتحدي الوصول وقبول الوصول ورفض الوصول، فإن المنطق هو نفسه تماما، ولكن من المهم تذكر أنه يجب إستخدام مصدق الطلب، والذي يتم توفيره في حزمة طلب الوصول السابقة.

معلومات ذات صلة

- المعيار RFC 2865
- المعيار RFC 2866
- المعيار RFC 3579
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).