نظرة عامة على Kerberos - دمة المصادقة لأنظمة الشبكة المفتوحة

المحتويات

المقدمة

في بيئة حوسبة الشبكة المفتوحة، لا يمكن الوثوق بمحطة العمل لتعريف مستخدميها بشكل صحيح لخدمات الشبكة. يوفر Kerberos أسلوبًا بديلاً يتم من خلاله استخدام خدمة مصادقة جهة خارجية موثوق بها للتحقق من هويات المستخدمين. تُقدّم هذه الورقة لمحة عامة عن نموذج مصادقة Kerberos كما تم تنفيذه في مشروع Athena التابع لمعهد ماساتشوستس للتكنولوجيا. يصف البروتوكولات المُستخدمة من قِبل العملاء والخوادم وKerberos لتحقيق المصادقة. كما يصف إدارة قاعدة البيانات المطلوبة والنسخ المتماثل لها. يتم وصف طرق عرض Kerberos كما يراها المستخدم والمبرمج والمسؤول. أخيرًا، يتم منح دور Kerberos في صورة Athena الأكبر، جنبًا إلى جنب مع قائمة بالتطبيقات التي تستخدم حاليًا Kerberos لمصادقة المستخدم. نحن نصف إضافة مصادقة Kerberos إلى نظام ملفات شبكة Sun كدراسة حالة لدمج Kerberos مع تطبيق موجود بالفعل.

كتاب Kerberos

- جينيفر جي. شتاينر، مشروع أثينا، معهد ماساتشوستس للتكنولوجيا، كامبريدج، MA 02139، steiner@ATHENA.MIT.EDU
- كليفورد نيومان، قسم علوم الحاسوب، FR-35، جامعة واشنطن، سياتل، WA 98195، bcn@CS.WASHINGTON.EDU. كان كليفورد نيومان عضوا في موظفي مشروع أثينا خلال مرحلة التصميم والتنفيذ الأولي ل Kerberos.
- جيفري إي. شيلر، مشروع أثينا، معهد ماساتشوستس للتكنولوجيا، كامبريدج، MA 02139، jis@ATHENA.MIT.EDU

مقدمة إلى Kerberos

تقدم هذه الورقة نظرة عامة على Kerberos، وهو نظام مصادقة صممه كل من ميلر ونويمان. لبيئات الحوسبة المفتوحة عبر الشبكة، وتصف تجربتنا باستخدامها في مشروع MIT Athena. في قسم التحفيز، نشرح لماذا يلزم نموذج مصادقة جديد للشبكات المفتوحة، وما هي متطلباته. يسرد قسم ما هو Kerberos؟ مكونات برنامج Kerberos ويصف كيفية تفاعلها في توفير خدمة المصادقة. في قسم أسماء Kerberos، نصف نظام تسمية Kerberos.

كيفية عمل Kerberos يمثل اللبنات الأساسية لمصادقة Kerberos - التذكرة والمصدق. وهذا يؤدي إلى مناقشة بروتوكولي المصادقة: المصادقة الأولية لمستخدم إلى Kerberos (مماثل لتسجيل الدخول)، وبروتوكول المصادقة المتبادلة لمستهلك محتمل ومنتج محتمل لخدمة شبكة.

يتطلب Kerberos قاعدة بيانات من المعلومات حول عملائه، يصف قسم قاعدة بيانات Kerberos قاعدة البيانات وإدارتها والبروتوكول لتعديلها. يصف Kerberos من الخارج في قسم Kerberos قارن إلى مستخدميه، مبرمجي التطبيقات، والإداريين. في قسم الصورة الأكبر، نصف كيف يتناسب مشروع Athena Kerberos مع بقية بيئة أثينا. ونصف أيضا التفاعل بين مجالات أو مجالات مختلفة لمصادقة Kerberos؛ وفي حالتنا، العلاقة بين مشروع Athena Kerberos ومشروع Kerberos الذي يعمل في مختبر MIT لعلوم الكمبيوتر.

وفي قسم القضايا والمشاكل المفتوحة، نذكر المسائل والمشاكل المفتوحة التي لم تحل بعد. يعطي القسم الأخير الحالة الحالية ل Kerberos في مشروع Athena. في الملحق، نقدم وصفا تفصيليا لكيفية تطبيق Kerberos على خدمة ملف الشبكة لمصادقة المستخدمين الذين يرغبون في الوصول إلى أنظمة الملفات البعيدة.

مفاهيم Kerberos

في هذه الورقة، نستخدم مصطلحات قد تكون غامضة، جديدة على القارئ، أو مستخدمة بشكل مختلف في مكان آخر. أدناه نعلن إستخدامنا لهذه المصطلحات.

المستخدم، العميل، الخادم—حسب المستخدم، فنحن نعني الإنسان الذي يستخدم برنامجا أو خدمة. الزبون يستخدم

أيضا شيئا ما، لكن ليس بالضرورة شخصا، يمكن أن يكون برنامجا. تتألف تطبيقات الشبكة عادة من جزأين، أحدهما يعمل على جهاز واحد ويطلب خدمة عن بعد، والآخر يعمل على الجهاز البعيد ويقوم بهذه الخدمة. ونستدعوهم إلى جانب العميل وجانب الخادم من التطبيق، على التوالي. غالبا ما يتصل العميل بالخادم نيابة عن مستخدم.

كل كيان يستخدم نظام Kerberos، سواء كان مستخدما أو خادم شبكة، هو عميل بمعنى واحد، نظرا لأنه يستخدم خدمة Kerberos. حتى نميز عملاء Kerberos من عملاء الخدمات الأخرى، نستخدم المصطلح الرئيسي للإشارة إلى مثل هذا الكيان. لاحظ أن أساسي Kerberos يمكن أن يكون مستخدم أو خادم. (نحن نصف تسمية مبادئ Kerberos في قسم لاحق.)

الخدمة مقابل الخادم — نستخدم الخدمة كمواصفات مجردة لبعض الإجراءات التي سيتم تنفيذها. وتسمى العملية التي تنفذ تلك الإجراءات بخادم. وفي وقت معين، قد تكون هناك عدة خوادم (تعمل عادة على أجهزة مختلفة) تقوم بتنفيذ خدمة معينة. على سبيل المثال، في Athena يوجد خادم BSD UNIX Rlogin يعمل على كل من آلاتنا المستخدمة في الوقت.

المفتاح، المفتاح الخاص، كلمة السر—Kerberos يستخدم تشفير مفتاح خاص. يتم تعيين رقم كبير لكل مدير Kerberos، وهو مفتاحه الخاص، والمعروف فقط لهذا المدير و Kerberos. في حالة مستخدم ما، يكون المفتاح الخاص نتيجة لدالة أحادية الإتجاه مطبقة على كلمة مرور المستخدم. نستخدم المفتاح كاختزال للمفتاح الخاص.

بيانات الاعتماد—لسوء الحظ، لهذه الكلمة معنى خاص لكل من نظام ملفات شبكة Sun ونظام Kerberos. نصرح صراحة ما إذا كنا نعني مسوغات NFS أو مسوغات Kerberos، وإلا فإن المصطلح يستخدم بالمعنى العادي للغة الإنجليزية.

Master و Slave—من الممكن تشغيل برنامج مصادقة Kerberos على أكثر من جهاز. ومع ذلك، هناك دائما نسخة نهائية واحدة فقط من قاعدة بيانات Kerberos. الآلة التي تضم قاعدة البيانات هذه تسمى الماكنة الرئيسية، أو الماجستير فقط. وقد تملك آلات أخرى نسخا للقراءة فقط من قاعدة بيانات كربيروس، وهذه تدعى عبيدا.

الدافع وراء Kerberos

في بيئة الحوسبة الشخصية غير المتصلة بشبكات، يمكن حماية الموارد والمعلومات من خلال تأمين الكمبيوتر الشخصي بشكل فعلي. في بيئة الحوسبة ذات الوقت، يحمي نظام التشغيل المستخدمين من بعضهم البعض ويتحكم في الموارد. لتحديد ما يمكن لكل مستخدم قراءته أو تعديله، من الضروري أن يقوم النظام الزمني بتعريف كل مستخدم. ويتم تحقيق ذلك عند تسجيل دخول المستخدم.

في شبكة من المستخدمين الذين يحتاجون إلى خدمات من العديد من أجهزة الكمبيوتر المنفصلة، هناك ثلاثة طرق يمكن أن يتبعها المرء للتحكم في الوصول: لا يمكن للمرء أن يفعل شيئا، ويعتمد على الجهاز الذي سجل المستخدم الدخول إليه لمنع الوصول غير المصرح به إليه؛ ويمكن للمرء أن يطلب من المضيف أن يثبت هويته، ولكنه يثق في كلمة المضيف فيما يتعلق بهوية المستخدم؛ أو يمكن للمرء أن يطلب من المستخدم إثبات هويته/هويته لكل خدمة مطلوبة.

وفي بيئة مغلقة تخضع فيها كل الآلات لرقابة صارمة، يمكن للمرء أن يستخدم النهج الأول. عندما تسيطر المنظمة على جميع البيئات المضيفة التي تتواصل عبر الشبكة، يكون هذا نهجا معقولا.

وفي بيئة أكثر انفتاحا، قد لا يثق المرء بشكل انتقائي إلا في البلدان المضيفة الخاضعة لسيطرة المنظمة. وفي هذه الحالة، يجب أن يطلب من كل مضيف إثبات هويته. تستخدم برامج rlogin و rsh هذا النهج. في هذه البروتوكولات، تتم المصادقة عن طريق التحقق من عنوان الإنترنت الذي تم إنشاء اتصال منه.

في بيئة أثينا، يجب أن نكون قادرين على تلبية الطلبات من البيئات المضيفة التي لا تخضع لرقابة المنظمة. يستطيع المستخدمون التحكم التام بمحطات العمل الخاصة بهم، حيث يمكنهم إعادة تشغيلها أو جلبها بمفردهم أو حتى التمهيد للحصول على الأشرطة الخاصة بهم. وعلى هذا النحو، يجب اتباع النهج الثالث؛ ويجب أن يثبت المستعمل هويته لكل خدمة مرغوبة. يجب أن يثبت الخادم هويته أيضا. لا يكفي تأمين المضيف ماديا الذي يشغل خادم الشبكة؛ فقد يكون هناك شخص آخر على الشبكة يتخفى على أنه الخادم المحدد.

وتضع بيئتنا عدة متطلبات على آلية تحديد الهوية. أولا، يجب أن تكون آمنة. ويجب أن يكون التحايل عليه صعبا بما فيه

الكفاية بحيث لا يجد المهاجم المحتمل آلية المصادقة هي الرابط الضعيف. لا يجب أن يكون الشخص الذي يراقب الشبكة قادرا على الحصول على المعلومات اللازمة لانتحال صفة مستخدم آخر. ثانيا، يجب ان يكون موثوقا به. يعتمد الوصول إلى العديد من الخدمات على خدمة المصادقة. وإذا لم يكن نظام الخدمات ككل موثوقا به، فلن يكون كذلك. ثالثا، لابد وأن يكون هذا التوجه شفافا. من الناحية المثالية، لا ينبغي للمستخدم أن يكون على علم بحدوث المصادقة. وأخيرا، لابد أن يكون قابلا للتطوير. تستطيع العديد من الأنظمة التواصل مع مضيفيها في أثينا. ولن تدعم كل هذه العوامل آليتنا، ولكن البرامج لا ينبغي لها أن تنكسر إذا انكسرت.

Kerberos هو نتيجة عملنا للوفاء بالمتطلبات المذكورة أعلاه. عندما يصل المستخدم إلى محطة عمل فإنه يقوم بتسجيل الدخول. وبقدر ما يمكن للمستخدم معرفة ذلك، فإن هذا التعريف الأولي يكفي لإثبات هويتها لجميع خوادم الشبكة المطلوبة طوال مدة جلسة تسجيل الدخول. يعتمد أمان Kerberos على أمان العديد من خوادم المصادقة، ولكن ليس على النظام الذي يقوم المستخدمون بتسجيل الدخول منه أو على أمان الخوادم الطرفية التي سيتم إستخدامها. يوفر خادم المصادقة لمستخدم تتم مصادقته بشكل صحيح مع طريقة لإثبات هويته/هويته للخوادم المنتشرة عبر الشبكة.

تعد المصادقة كتلة أساسية لبيئة آمنة متصلة عبر شبكة. على سبيل المثال، إذا كان الخادم يعرف هوية العميل بشكل مؤكد، فيمكنه أن يقرر ما إذا كان سيقدم الخدمة، وما إذا كان ينبغي منح المستخدم امتيازات خاصة، ومن الذي ينبغي أن يتلقى فاتورة الخدمة، وما إلى ذلك. بمعنى آخر، يمكن إنشاء أنظمة التخويل والمحاسبة فوق المصادقة التي يوفرها Kerberos، مما ينتج عنه تأمين مكافئ لجهاز الكمبيوتر الشخصي الوحيد أو نظام توجيه الوقت.

ما هو Kerberos؟

Kerberos هي خدمة مصادقة موثوق بها من قبل طرف ثالث استنادا إلى النموذج الذي قدمه كل من Needham و Schroeder. وهو جدير بالثقة بمعنى أن كل عميل من عملائه يعتقد أن حكم كيربيروس على هوية كل من عملائه الآخرين كان دقيقا. تمت إضافة الطوابع الزمنية (أرقام كبيرة تمثل التاريخ والوقت الحاليين) إلى النموذج الأصلي للمساعدة في اكتشاف إعادة التشغيل. تحدث إعادة التشغيل عند سرقة رسالة من الشبكة ثم إلغائها لاحقا. للحصول على وصف أكثر اكتمالا لإعادة التشغيل، ومسائل أخرى للمصادقة، راجع Voydock و Kent.

ماذا يفعل Kerberos؟

يحتفظ Kerberos بقاعدة بيانات لعملائه ومفاتيحهم الخاصة. المفتاح الخاص هو رقم كبير معروف فقط ل Kerberos والعميل الذي ينتمي إليه. في حالة ما إذا كان العميل مستخدما، فإنها كلمة مرور مشفرة. خدمات الشبكة التي تتطلب سجل المصادقة مع Kerberos، كما هو الحال مع العملاء الذين يرغبون في إستخدام هذه الخدمات. يتم التفاوض على المفاتيح الخاصة عند التسجيل.

ولأن Kerberos يعرف هذه المفاتيح الخاصة، يمكنه إنشاء رسائل تقنع أحد العملاء بأن العميل الآخر هو حقا من يدعي أنه. كما يقوم Kerberos بإنشاء مفاتيح خاصة مؤقتة، تسمى مفاتيح الجلسة، والتي يتم تقديمها إلى عميلين ولا أحد آخر. يمكن إستخدام مفتاح جلسة عمل لتشفير الرسائل بين طرفين.

يوفر Kerberos ثلاثة مستويات متميزة من الحماية. ويحدد مبرمج التطبيق ما هو المناسب، وفقا لمتطلبات الطلب. على سبيل المثال، تتطلب بعض التطبيقات فقط أن يتم تأسيس الأصالة عند بدء اتصال شبكة، ويمكن أن تفترض أن رسائل أخرى من عنوان شبكة معين تنشأ من الطرف المصدق عليه. يستخدم نظام ملفات الشبكة المصادق الخاص بنا هذا المستوى من الأمان.

تتطلب التطبيقات الأخرى مصادقة كل رسالة، ولا تهتم بما إذا كان محتوى الرسالة قد تم الإفصاح عنه أم لا. لهذه، توفر Kerberos رسائل آمنة. ومع ذلك، يتم توفير مستوى أعلى من الأمان بواسطة الرسائل الخاصة، حيث لا يتم مصادقة كل رسالة فقط، بل يتم تشفيرها أيضا. على سبيل المثال، يتم إستخدام الرسائل الخاصة من قبل خادم Kerberos نفسه لإرسال كلمات المرور عبر الشبكة.

مكونات برنامج Kerberos

يشمل تنفيذ أثينا عدة وحدات:

- مكتبة تطبيقات Kerberos
- مكتبة تشفير
- مكتبة قواعد البيانات
- برامج إدارة قواعد البيانات
- خادم الإدارة
- خادم المصادقة
- برنامج نشر DB
- برامج المستخدم
- التطبيقات

توفر مكتبة تطبيقات Kerberos واجهة لعملاء التطبيقات وخوادم التطبيقات. كما يحتوي، من بين أمور أخرى، على موجهات لإنشاء طلبات المصادقة أو قراءتها، وعلى موجهات إنشاء رسائل آمنة أو خاصة.

يعتمد التشفير في Kerberos على معيار DES، وهو معيار تشفير البيانات. تقوم مكتبة التشفير بتنفيذ تلك الروتين. يتم توفير العديد من طرق التشفير، مع المفاضلة بين السرعة والأمان. كما يتم توفير ملحق لوضع Cisco DES Cipher Block Sequence (CBC)، يسمى وضع Deployment CBC. في CBC، يتم نشر خطأ فقط من خلال الكتلة الحالية للشفرة، بينما في PCBC، يتم نشر الخطأ عبر الرسالة. وهذا من شأنه أن يجعل الرسالة بالكامل بلا فائدة إذا وقع خطأ ما، وليس مجرد جزء منها. مكتبة التشفير هي وحدة مستقلة، ويمكن إستبدالها بعمليات تنفيذ DES أخرى أو مكتبة تشفير مختلفة.

ومن الوحدات الأخرى القابلة للاستبدال نظام إدارة قواعد البيانات. يستخدم تنفيذ Athena الحالي لمكتبة قواعد البيانات NDBM، على الرغم من إستخدام Ingres في الأصل. كما يمكن إستخدام مكتبات إدارة قواعد بيانات أخرى.

إن إحتياجات قاعدة بيانات Kerberos واضحة، حيث يتم الاحتفاظ بسجل لكل مدير يحتوي على الاسم، والمفتاح الخاص، وتاريخ انتهاء صلاحية الأصل، بالإضافة إلى بعض المعلومات الإدارية. (تاريخ انتهاء الصلاحية هو التاريخ الذي لم يعد الإدخال صالحا بعده. وهو معد عادة لبضع سنوات في المستقبل عند التسجيل).

يتم الاحتفاظ بمعلومات المستخدم الأخرى، مثل الاسم الحقيقي ورقم الهاتف وما إلى ذلك، بواسطة خادم آخر، Hesiod Nameserver. بهذه الطريقة، يمكن معالجة المعلومات الحساسة، أي كلمات المرور، بواسطة Kerberos، باستخدام تدابير أمنية عالية إلى حد ما، بينما يتم التعامل مع المعلومات غير الحساسة التي يحتفظ بها Hesiod بشكل مختلف، على سبيل المثال، يمكن إرسالها دون تشفير عبر الشبكة.

تستخدم خوادم Kerberos مكتبة قاعدة البيانات، وكذلك الأدوات الخاصة بإدارة قاعدة البيانات.

يوفر خادم الإدارة (أو خادم KDBM) واجهة شبكة للقراءة والكتابة لقاعدة البيانات. قد يتم تشغيل جانب العميل من البرنامج على أي جهاز على الشبكة. ومع ذلك، يجب تشغيل جانب الخادم على الجهاز الذي يحتوي على قاعدة بيانات Kerberos لإجراء تغييرات على قاعدة البيانات.

من ناحية أخرى، يقوم خادم المصادقة (أو خادم Kerberos) بعمليات قراءة فقط على قاعدة بيانات Kerberos، وهي مصادقة الأساسيات وإنشاء مفاتيح الجلسة. نظرا لأن هذا الخادم لا يقوم بتعديل قاعدة بيانات Kerberos، فقد يتم تشغيلها على جهاز يحتوي على نسخة للقراءة فقط من قاعدة بيانات Kerberos الرئيسية.

يقوم برنامج نشر قاعدة البيانات بإدارة النسخ المتماثل لقاعدة بيانات Kerberos. من الممكن الحصول على نسخ من قاعدة البيانات على عدة أجهزة مختلفة، مع نسخة من خادم المصادقة تعمل على كل جهاز. كل من هذه الآلات المستعملة يستلم تحديث قاعدة بيانات Kerberos من الآلة الرئيسية في فترات زمنية معينة.

وأخيرا، هناك برامج للمستخدم النهائي لتسجيل الدخول إلى Kerberos، وتغيير كلمة مرور Kerberos، وعرض تذاكر Kerberos أو تدميرها (يتم شرح التذاكر لاحقا).

أسماء Kerberos

يقوم جزء من مصادقة كيان بتسميته. عملية المصادقة هي التحقق من أن العميل هو الذي تم تسميته في الطلب. ما

الذي يتكون منه الاسم؟ في Kerberos، كل من المستخدمين والخوادم مسماة. وبقدر ما يتعلق الأمر بخادم المصادقة، فإنها مكافئة. يتكون الاسم من اسم أساسي ومثيل وعالم، يتم التعبير عنه باسم name.instance@realm.

الاسم الأساسي هو اسم المستخدم أو الخدمة. يستخدم المثيل للتمييز بين التباينات على الاسم الأساسي. بالنسبة للمستخدمين، قد يتطلب المثيل امتيازات خاصة، مثل مثيلات "الجذر" أو "المسؤول". بالنسبة للخدمات في بيئة Athena، يكون المثيل عادة هو اسم الجهاز الذي يعمل عليه الخادم. على سبيل المثال، تحتوي خدمة rlogin على مثيلات مختلفة على مضيفين مختلفين: rlogin.priam هو خادم rlogin على المضيف المسمى priam. تعد تذكرة Kerberos صالحة فقط لخادم واحد مسمى. وعلى هذا النحو، يلزم وجود تذكرة منفصلة للوصول إلى مثيلات مختلفة من نفس الخدمة. النطاق هو اسم كيان إداري يحتفظ ببيانات المصادقة. على سبيل المثال، قد يكون لكل مؤسسة مختلفة جهاز Kerberos خاص بها، والذي يشتمل على قاعدة بيانات مختلفة. لديهم عوائد كيربيروس مختلفة. (تتم مناقشة الأمور بمزيد من التفصيل في التفاعل مع كيربري الأخرى).

كيفية عمل Kerberos

يصف هذا القسم بروتوكولات مصادقة Kerberos. وكما ذكر أعلاه، فإن نموذج مصادقة Kerberos يستند إلى بروتوكول التوزيع الأساسي Needham و Schroeder. عندما يطلب المستخدم خدمة ما، يجب تحديد هويته. وللقيام بذلك، تقدم تذكرة إلى الخادم، مع إثبات أن التذكرة صدرت في الأصل إلى المستخدم، وليس مسروقة. هناك ثلاث مراحل للمصادقة من خلال Kerberos. في المرحلة الأولى، يحصل المستخدم على بيانات اعتماد ليتم إستخدامها لطلب الوصول إلى خدمات أخرى. في المرحلة الثانية، يطلب المستخدم المصادقة لخدمة معينة. في المرحلة النهائية، يقدم المستخدم بيانات الاعتماد هذه إلى الخادم النهائي.

بيانات اعتماد Kerberos

هناك نوعان من بيانات الاعتماد المستخدمة في نموذج مصادقة Kerberos: التذاكر والمصادقة. يعتمد كل منهما على تشفير المفاتيح الخاصة، ولكن يتم تشفيرها باستخدام مفاتيح مختلفة. تستخدم التذكرة لتمرير هوية الشخص الذي تم إصدار التذكرة له بين خادم المصادقة والخادم الطرفي بشكل آمن. وتمرر التذكرة أيضا معلومات يمكن إستخدامها للتأكد من ان الشخص الذي يستعمل التذكرة هو الشخص نفسه الذي صدرت اليه. ويحتوي المصدق على المعلومات الإضافية التي تثبت عند مقارنتها بتلك الواردة في التذكرة أن العميل الذي يقدم التذكرة هو نفسه الذي صدرت له التذكرة.

فالتذكرة مفيدة لخادم واحد وزبون واحد. وهو يحتوي على اسم الخادم واسم العميل وعنوان الإنترنت الخاص بالعميل وطابع زمني ودورة حياة ومفتاح جلسة عشوائية. يتم تشفير هذه المعلومات باستخدام مفتاح الخادم الذي سيتم إستخدام التذكرة من أجله. وبمجرد إصدار التذكرة، يمكن إستخدامها عدة مرات من قبل العميل المسمى للوصول إلى الخادم المسمى، إلى أن تنتهي صلاحية التذكرة. لاحظ أنه نظرا لأنه يتم تشفير التذكرة في مفتاح الخادم، فمن الأمان السماح للمستخدم بتمرير التذكرة إلى الخادم دون الحاجة إلى القلق بشأن قيام المستخدم بتعديل التذكرة.

وعلى عكس التذكرة، يمكن إستخدام المصدق مرة واحدة فقط. يجب إنشاء خدمة جديدة في كل مرة يريد فيها العميل إستخدام خدمة. لا يمثل هذا مشكلة لأن العميل قادر على إنشاء المصدق نفسه. يحتوي المصدق على اسم العميل وعنوان IP لمحطة العمل ووقت محطة العمل الحالي. يتم تشفير المصدق في مفتاح جلسة العمل الذي يعد جزءا من التذكرة.

احصل على تذكرة Kerberos الأولية

عندما يصل المستخدم إلى محطة عمل، يمكن لمقطع واحد فقط من المعلومات إثبات هويته، وهو كلمة مرور المستخدم. وقد تم تصميم التبادل الأولي مع خادم المصادقة لتقليل فرصة أختراق كلمة المرور، مع عدم السماح في الوقت نفسه لمستخدم بالمصادقة على نفسه بشكل صحيح دون معرفة كلمة المرور هذه. يبدو أن عملية تسجيل الدخول للمستخدم هي نفسها تسجيل الدخول إلى نظام مشاركة الوقت. ولكن وراء الكواليس، يكون الامر مختلفا تماما.

تم مطالبة المستخدم باسم المستخدم الخاص به. وبمجرد إدخالها، يتم إرسال طلب إلى خادم المصادقة يحتوي على

اسم المستخدم واسم خدمة خاصة تعرف باسم خدمة منح التذاكر.

يتحقق خادم المصادقة من علمه بالعميل. إذا كان الأمر كذلك، فإنه يقوم بإنشاء مفتاح جلسة عمل عشوائي سيتم إستخدامه فيما بعد بين العميل والخادم الذي يمنح التذكرة. ثم يقوم بإنشاء تذكرة للخادم الذي يمنح التذكرة والتي تحتوي على اسم العميل، اسم الخادم الذي يمنح التذكرة، الوقت الحالي، العمر الافتراضي للتذكرة، عنوان IP الخاص بالعميل، ومفتاح الجلسة العشوائية الذي تم إنشاؤه للتو. وهذا كله مشفر في مفتاح لا يعرف إلا لخادم منح التذاكر وخادم المصادقة.

ثم يرسل خادم المصادقة البطاقة مع نسخة من مفتاح الجلسة العشوائية وبعض المعلومات الإضافية مرة أخرى إلى العميل. يتم تشفير هذه الاستجابة في المفتاح الخاص للعميل، والمعروف فقط ل Kerberos والعميل، والذي يتم اشتقاقه من كلمة مرور المستخدم.

وبمجرد تلقي العميل للرد، يطلب من المستخدم كلمة المرور الخاصة به. يتم تحويل كلمة المرور إلى مفتاح DES وتستخدم لفك تشفير الاستجابة من خادم المصادقة. يتم تخزين التذكرة ومفتاح الجلسة، بالإضافة إلى بعض المعلومات الأخرى، للاستخدام المستقبلي، ويتم مسح كلمة مرور المستخدم ومفتاح DES من الذاكرة.

وبمجرد إتمام عملية التبادل، فإن محطة العمل تمتلك المعلومات التي يمكنها إستخدامها لإثبات هوية المستخدم مدى الحياة للتذكرة الممنوحة. طالما لم يتم العبث بالبرامج الموجودة على محطة العمل من قبل، لا توجد أية معلومات تسمح لشخص آخر بانتحال صفة المستخدم بعد انتهاء مدة صلاحية التذكرة.

طلب خدمة Kerberos

وفي الوقت الحالي، دعونا نتظاهر بأن المستخدم لديه بالفعل تذكرة للخادم المرغوب فيه. للحصول على حق الوصول إلى الخادم، يقوم التطبيق بإنشاء مصدق يحتوي على اسم العميل وعنوان IP، والوقت الحالي. وبعد ذلك يتم تشفير المصدق في مفتاح جلسة العمل الذي تم إستلامه مع التذكرة الخاصة بالخادم. وبعد ذلك يرسل العميل المصدق مع التذكرة إلى الخادم بطريقة محددة بواسطة التطبيق الفردي.

وبمجرد إستلام المصدق والتذكرة بواسطة الخادم، يقوم الخادم بفك تشفير التذكرة، ويستخدم مفتاح جلسة العمل المضمن في التذكرة لفك تشفير المصدق، ويقارن المعلومات الواردة في التذكرة بتلك الموجودة في المصدق وعنوان IP الذي تم إستلام الطلب منه والوقت الحالي. في حالة تطابق كل شيء، فإنه يسمح بمتابعة الطلب.

يفترض أن الساعات تتزامن مع بعضها خلال عدة دقائق. إذا كان الوقت في الطلب بعيدا جدا في المستقبل أو في الماضي، فإن الخادم يتعامل مع الطلب كمحاولة لإعادة تشغيل طلب سابق. كما يسمح للخادم بتعقب كافة الطلبات السابقة ذات الطوابع الزمنية التي لا تزال صالحة. ولمزيد من إحباط هجمات إعادة التشغيل، يمكن تجاهل طلب ورد بنفس التذكرة والطابع الزمني اللذين سبق تلقيهما.

وأخيرا، إذا قام العميل بتحديد رغبته في أن يثبت الخادم هويته أيضا، فسيقوم الخادم بإضافة واحد إلى الطابع الزمني الذي أرسله العميل في المصدق، ويقوم بتشفير النتيجة في مفتاح جلسة العمل، وإرسال النتيجة مرة أخرى إلى العميل.

في نهاية هذا التبادل، يكون الخادم متأكدا من أن العميل، وفقا ل Kerberos، هو من يقول عنه. في حالة حدوث مصادقة متبادلة، يكون العميل مقتنعا أيضا بأن الخادم أصلي. علاوة على ذلك، يشترك العميل والخادم في مفتاح لا يعرفه أي شخص آخر، ويمكنهما أن يفترضا بأمان أن رسالة حديثة بشكل معقول مشفرة في ذلك المفتاح نشأت مع الطرف الآخر.

الحصول على تذاكر خادم Kerberos

تذكر أن التذكرة تكون جيدة لخادم واحد فقط. وعلى هذا النحو، من الضروري الحصول على تذكرة منفصلة لكل خدمة يريد العميل إستخدامها. ويمكن الحصول على تذاكر للخوادم الفردية من خدمة منح التذاكر. ونظرا لأن خدمة منح التذاكر هي نفسها خدمة، فإنها تستخدم بروتوكول الوصول إلى الخدمة المذكور في القسم السابق.

عندما يتطلب أحد البرامج تذكرة لم يتم طلبها بالفعل، فإنه يرسل طلبا إلى الخادم الذي يمنح التذكرة. يحتوي الطلب على اسم الخادم المطلوب له تذكرة، بالإضافة إلى تذكرة منح التذكرة ومصدق مضمن كما هو موضح في القسم

السابق.

ثم يتحقق الخادم الذي يمنح التذاكر من المصدق والتذكرة التي تمنح التذاكر كما هو موضح أعلاه. إن كان صحيحا، يقوم الخادم الذي يمنح التذكرة بإنشاء مفتاح جلسة عمل عشوائي جديد يتم إستخدامه بين العميل والخادم الجديد. ثم يقوم بإنشاء تذكرة للخادم الجديد تحتوي على اسم العميل واسم الخادم والوقت الحالي وعنوان IP الخاص بالعميل ومفتاح الجلسة الجديد الذي تم إنشاؤه للتو. وفترة صلاحية التذكرة الجديدة هي الحد الأدنى من العمر المتبقي لتذكرة منح التذكرة والقصير للخدمة.

ثم يرسل الخادم الذي يمنح التذكرة التذكرة، مع مفتاح جلسة العمل ومعلومات أخرى، مرة أخرى إلى العميل. ولكن هذه المرة، يشفر الرد في مفتاح جلسة العمل الذي كان جزءا من تذكرة منح التذاكر. بهذه الطريقة، لا توجد حاجة لأن يقوم المستخدم بإدخال كلمة المرور الخاصة به مرة أخرى.

قاعدة بيانات Kerberos

حتى هذه النقطة، ناقشنا العمليات التي تتطلب الوصول للقراءة فقط إلى قاعدة بيانات Kerberos. ويتم تنفيذ هذه العمليات بواسطة خدمة المصادقة، والتي يمكن تشغيلها على الأجهزة الرئيسية وأجهزة العبيد.

في هذا القسم، نناقش العمليات التي تتطلب الوصول للكتابة إلى قاعدة البيانات. يتم تنفيذ هذه العمليات بواسطة خدمة الإدارة، التي تسمى خدمة إدارة قاعدة بيانات Kerberos (KDBM). ينص التطبيق الحالي على أنه لا يمكن إجراء تغييرات إلا على قاعدة بيانات Kerberos الرئيسية؛ فالنسخ المستنسخة المستنسخة تكون للقراءة فقط. لذلك، يمكن تشغيل خادم KDBM فقط على جهاز Kerberos الرئيسي.

لاحظ أنه، بينما لا يزال من الممكن أن تحدث المصادقة (على العبيد)، لا يمكن خدمة طلبات الإدارة إذا كان الجهاز الرئيسي معطلا. ومن واقع خبرتنا، لم يطرح ذلك مشكلة، لأن طلبات الإدارة نادرة.

يعالج KDBM طلبات المستخدمين لتغيير كلمات المرور الخاصة بهم. جانب العميل من هذا البرنامج، والذي يرسل الطلبات إلى KDBM عبر الشبكة، هو برنامج kpasswd. كما يقبل KDBM الطلبات من مسؤولي Kerberos، الذين قد يضيفون مبادئ إلى قاعدة البيانات، بالإضافة إلى تغيير كلمات المرور للأساسيات الموجودة. وجانب العميل من برنامج الإدارة، الذي يرسل أيضا طلبات إلى KDBM عبر الشبكة، هو برنامج Kadmin.

خادم KDBM

يقبل خادم KDBM طلبات إضافة أساسيات إلى قاعدة البيانات أو تغيير كلمات المرور للأساسيات الموجودة. وهذه الخدمة فريدة من نوعها لأن خدمة منح التذاكر لن تصدر تذاكر لها. وبدلا من ذلك، يجب إستخدام خدمة المصادقة نفسها (نفس الخدمة التي يتم إستخدامها للحصول على تذكرة لمنح التذكرة). الغرض من هذا هو أن يطلب من المستخدم إدخال كلمة مرور. وإذا لم يكن الأمر كذلك، فإنه إذا ترك المستخدم محطة العمل الخاصة به دون مراقبة، فيمكن للمارة أن تمشي وتغير كلمة المرور الخاصة بها/بكلمة المرور الخاصة به بالنسبة لهم، وهو ما يجب منعه. وعلى نحو مماثل، إذا ترك المسؤول محطة العمل الخاصة به غير خاضعة للحراسة، فيمكن للمارة تغيير أي كلمة مرور في النظام.

عندما يتلقى خادم KDBM طلبا، فإنه يخوله بمقارنة الاسم الأساسي المصدق عليه لطالب التغيير مع الاسم الأساسي لهدف الطلب. إذا كانا متشابهين، فيتم السماح بالطلب. إذا لم تكن متطابقة، يستشير خادم KDBM قائمة تحكم في الوصول (مخزنة في ملف على نظام Kerberos الرئيسي). إذا تم العثور على الاسم الأساسي للطالب في هذا الملف، يتم السماح بالطلب، وإلا يتم رفضه.

وفقا للصيغة، لا تظهر الأسماء ذات المثيل NULL (المثيل الافتراضي) في ملف قائمة التحكم بالوصول؛ وبدلا من ذلك، يتم إستخدام مثيل مسؤول. لذلك، لكي يصبح المستخدم مسؤولا عن Kerberos، يجب إنشاء مثيل مسؤول لاسم المستخدم هذا، وإضافته إلى قائمة التحكم في الوصول. يسمح هذا الإتفاقية للمسؤول باستخدام كلمة مرور مختلفة لإدارة Kerberos ثم يتم إستخدامها لتسجيل الدخول العادي.

يتم تسجيل جميع الطلبات إلى برنامج KDBM، سواء كان مسموحا بها أو مرفوضة.

برامج الكادمين والكباسود

يستخدم مسؤولو Kerberos برنامج Kadmin لإضافة مبادئ إلى قاعدة البيانات أو تغيير كلمات المرور للأساسيات الموجودة. يجب أن يقوم المسؤول بإدخال كلمة المرور لاسم مثيل المسؤول الخاص به عند إستدعاء برنامج Kadmin. تستخدم كلمة المرور هذه لجلب تذكرة لخادم KDBM.

يمكن للمستخدمين تغيير كلمات مرور Kerberos الخاصة بهم باستخدام برنامج kpasswd. مطلوب منهم إدخال كلمة المرور القديمة عند إستدعاء البرنامج. تستخدم كلمة المرور هذه لجلب تذكرة لخادم KDBM.

النسخ المتماثل لقاعدة بيانات Kerberos

يحتوي كل مجال Kerberos على جهاز Kerberos رئيسي، والذي يحتوي على النسخة الرئيسية لقاعدة بيانات المصادقة. ويمكن (وإن لم يكن ذلك ضروريا) الحصول على نسخ إضافية للقراءة فقط من قاعدة البيانات المتعلقة بآلات الرقيق في أماكن أخرى من النظام. وتتمثل مزايا الحصول على نسخ متعددة من قاعدة البيانات في الميزات التي عادة ما يستشهد بها للنسخ المتماثل: توافر أعلى وأداء أفضل. وإذا تعطلت الآلة الرئيسية، يمكن تحقيق المصادقة على إحدى آلات الرقيق. تؤدي القدرة على إجراء المصادقة على أي جهاز من الأجهزة المتعددة إلى تقليل احتمال حدوث إزدحام في الجهاز الرئيسي.

يؤدي الاحتفاظ بنسخ متعددة من قاعدة البيانات إلى ظهور مشكلة تناسق البيانات. وقد وجدنا أن الأساليب البسيطة جدا تكفي للتعامل مع عدم الاتساق. يتم إغراق قاعدة البيانات الرئيسية كل ساعة. وترسل قاعدة البيانات بكاملها إلى آلات الرقيق، التي تقوم بعد ذلك بتحديث قواعد بياناتها الخاصة. برنامج على المضيف الرئيسي، يدعى كبروب، يرسل التحديث إلى برنامج نظير، يدعى كبرود، يعمل على كل آلة من آلات العبيد. يرسل Kprop الأول المجموع الاختباري لقاعدة البيانات الجديدة التي على وشك إرسالها. يتم تشفير المجموع الاختباري في مفتاح قاعدة بيانات رئيسي Kerberos، الذي تمتلكه كل من أجهزة Kerberos الرئيسية والرقيق. ثم تنقل البيانات عبر الشبكة إلى KPROD الموجود على آلة الرقيق. يقوم خادم نشر العبيد بحساب المجموع الاختباري للبيانات التي إستلمتها، وإذا تطابقت مع المجموع الاختباري الذي تم إرساله بواسطة المدير، يتم إستخدام المعلومات الجديدة لتحديث قاعدة بيانات العبيد.

يتم تشفير جميع كلمات المرور في قاعدة بيانات Kerberos في مفتاح قاعدة البيانات الرئيسي لذلك، فإن المعلومات التي يتم تمريرها من رئيسي إلى تابع عبر الشبكة غير مفيدة لمقطع معلومات. غير أنه من الضروري أن يقبل العبيد المعلومات الواردة من المضيف الرئيسي فقط، وأن يتم اكتشاف التلاعب بالبيانات، وبالتالي المجموع الاختباري.

Kerberos من الخارج يبحث في

يصف هذا القسم Kerberos من وجهة النظر العملية، أولا كما يراها المستخدم، ثم من وجهة نظر مبرمج التطبيق، وأخيرا، من خلال مهام مسؤول Kerberos.

طريقة عرض العين لمستخدم Kerberos

إذا سارت الأمور على ما يرام، فلن يلاحظ المستخدم وجود Kerberos. أثناء تطبيق نظام UNIX، يتم الحصول على تذكرة منح التذاكر من Kerberos كجزء من عملية تسجيل الدخول. يعد تغيير كلمة مرور Kerberos الخاصة بالمستخدم جزءا من برنامج كلمة المرور. ويتم إتلاف تذاكر Kerberos تلقائيا عند تسجيل خروج المستخدم.

إذا إستمرت جلسة تسجيل الدخول الخاصة بالمستخدم لمدة أطول من مدة صلاحية تذكرة منح التذكرة (حاليا 8 ساعات)، سيلاحظ المستخدم وجود Kerberos لأنه في المرة التالية التي يتم فيها تنفيذ تطبيق مصدق من Kerberos، سيفشل. ستنتهي صلاحية تذكرة Kerberos الخاصة بها. وعند تلك النقطة، يمكن للمستخدم تشغيل برنامج Kinit للحصول على تذكرة جديدة للخادم الذي يمنح التذاكر. كما هو الحال عند تسجيل الدخول، يجب توفير كلمة مرور للحصول عليها. قد يفاجأ المستخدم الذي ينفذ أمر klist بدافع الفضول عن جميع التذاكر التي تم الحصول عليها بصمت نيابة عنه للحصول على خدمات تتطلب مصادقة Kerberos.

Kerberos من وجهة نظر المبرمج

غالبا ما يقوم أحد المبرمجين الذي يكتب تطبيق Kerberos بإضافة مصادقة إلى تطبيق شبكة موجود بالفعل يتكون من جانب عميل وخادم. نسمي هذه العملية "Kerberating" ببرنامج. يتضمن المسافات بين الحروف عادة إجراء مكالمة إلى مكتبة Kerberos لإجراء المصادقة عند الطلب الأولي للخدمة. وقد يتضمن أيضا إستدعاءات إلى مكتبة DES لتشفير الرسائل والبيانات التي يتم إرسالها فيما بعد بين عميل التطبيق وخادم التطبيق.

أكثر وظائف المكتبة إستخداما هي krb_mk_req من جانب العميل و krb_rd_req من جانب الخادم. يأخذ روتين krb_mk_req كمعلمات اسم ومثيل وعالم الخادم الهدف، الذي سيتم طلبه، وربما المجموع الاختباري للبيانات التي سيتم إرسالها. بعد ذلك يرسل العميل الرسالة التي تم إرجاعها بواسطة إستدعاء krb_mk_req عبر الشبكة إلى جانب الخادم الخاص بالتطبيق. عندما يستقبل الخادم هذه الرسالة، يقوم بإجراء مكالمة لروتين المكتبة krb_rd_req. ويصدر الروتين حكما بشأن صحة هوية المرسل المزعومة.

إذا كان التطبيق يتطلب أن تكون الرسائل التي يتم إرسالها بين العميل والخادم سرية، فيمكن حينئذ إجراء مكالمات المكتبة إلى krb_rd_priv) krb_mk_priv) لتشفير الرسائل (فك تشفيرها) في مفتاح جلسة العمل الذي يشترك فيه كلا الجانبين الآن.

وظيفة مسؤول Kerberos

تبدأ مهمة مسؤول Kerberos بتشغيل برنامج لتهيئة قاعدة البيانات. يجب تشغيل برنامج آخر لتسجيل الأساسيات الأساسية في قاعدة البيانات، مثل اسم مسؤول Kerberos مع مثيل مسؤول. يجب بدء تشغيل خادم مصادقة Kerberos وخادم الإدارة. وفي حالة وجود قواعد بيانات خاصة بالعبيد، يتعين على المسؤول أن يرتب لشروع برامج نشر تحديثات قاعدة البيانات من الرقيق إلى الرقيق بصورة دورية.

وبعد إتخاذ هذه الخطوات الأولية، يقوم المسؤول بالتلاعب بقاعدة البيانات عبر الشبكة، باستخدام برنامج KADMIN. ومن خلال هذا البرنامج، يمكن إضافة مبادئ جديدة وتغيير كلمات المرور.

وعلى وجه الخصوص، عند إضافة تطبيق Kerberos جديد إلى النظام، يجب على مسؤول Kerberos إتخاذ بعض الخطوات لتشغيله. يجب تسجيل الخادم في قاعدة البيانات، وتعيين مفتاح خاص (عادة ما يكون هذا مفتاحا عشوائيا يتم إنشاؤه تلقائيا). بعد ذلك، يجب إستخراج بعض البيانات (بما في ذلك مفتاح الخادم) من قاعدة البيانات وتثبيتها في ملف على جهاز الخادم. الملف الافتراضي هو /etc/srvtab. يستخدم روتين مكتبة krb_rd_req الذي تم استدعاؤه بواسطة الخادم (راجع القسم السابق) المعلومات الموجودة في هذا الملف لفك تشفير الرسائل التي تم إرسالها المشفرة في مفتاح الخادم الخاص. يقوم ملف /etc/srvtab بمصادقة الخادم ككلمة مرور مكتوبة في وحدة طرفية لمصادقة المستخدم.

يجب على مسؤول Kerberos أيضا التأكد من أن أجهزة Kerberos آمنة ماديا، ومن الحكمة أيضا الحفاظ على النسخ الاحتياطية لقاعدة البيانات الرئيسية.

الصورة الأكبر ل Kerberos

في هذا القسم، نقدم وصفا لكيفية توافق Kerberos مع بيئة Athena، بما في ذلك إستخدامها من قبل خدمات وتطبيقات الشبكة الأخرى، وكيف تتفاعل مع بيئة Kerberos البعيدة. وللاطلاع على وصف أكثر اكتمالا لبيئة أثينا، يرجى الرجوع إلى جي. دبليو. تريزي.

إستخدام خدمات الشبكة الأخرى ل Kerberos

تم تعديل العديد من تطبيقات الشبكة لاستخدام Kerberos. تحاول أوامر rlogin و rsh أولا المصادقة باستخدام Kerberos. يمكن للمستخدم الذي لديه تذاكر Kerberos صالحة تسجيل الدخول إلى جهاز Athena آخر دون الحاجة إلى إعداد ملفات .rhosts. في حالة فشل مصادقة Kerberos، ترجع البرامج إلى أساليبها المعتادة للتخويل، وفي هذه الحالة، تقوم ملفات .hosts.

لقد قمنا بتعديل بروتوكول مكتب البريد لاستخدام Kerberos للمصادقة على المستخدمين الذين يرغبون في إسترداد بريدهم الإلكتروني من "مكتب البريد". وقد طور مؤخرا برنامج لتوصيل الرسائل يدعى زيفير في أثينا، وهو يستخدم

كيربروس للمصادقة أيضا.

يستخدم برنامج تسجيل المستخدمين الجدد، المسمى "تسجيل"، كلا من نظام إدارة الخدمات (SMS) و Kerberos. من SMS، تحدد ما إذا كانت المعلومات التي تم إدخالها من قبل مستخدم Athena الجديد، مثل الاسم ورقم تعريف MIT، صحيحة أم لا. ثم يتم التحقق من Kerberos لمعرفة ما إذا كان اسم المستخدم المطلوب فريدا. إذا سارت الأمور على ما يرام، يتم عمل مدخل جديد على قاعدة بيانات Kerberos، يحتوي على اسم المستخدم وكلمة المرور.

للحصول على مناقشة تفصيلية حول إستخدام Kerberos لتأمين نظام ملف شبكة Sun، الرجاء الرجوع إلى الملحق.

التفاعل مع كيربري الأخرى

من المتوقع أن ترغب المؤسسات الإدارية المختلفة في إستخدام Kerberos لمصادقة المستخدم. ومن المتوقع أيضا أن يرغب المستخدمون في كثير من الحالات في إستخدام الخدمات في مؤسسة أخرى. يدعم Kerberos مجالات إدارية متعددة. تتضمن مواصفات الأسماء في Kerberos حقلا يسمى المجال. يحتوي هذا الحقل على اسم المجال الإداري الذي يجب مصادقة المستخدم بداخله.

يتم تسجيل الخدمات عادة في نطاق واحد ولن تقبل إلا بيانات الاعتماد التي يصدرها خادم المصادقة لذلك النطاق. يتم تسجيل المستخدم عادة في نطاق واحد (النطاق المحلي)، ولكن يمكن له/له الحصول على بيانات اعتماد صادرة عن نطاق آخر (النطاق البعيد)، بقوة المصادقة المقدمة من النطاق المحلي. تشير بيانات الاعتماد الصالحة في نطاق بعيد إلى المجال الذي تمت مصادقة المستخدم فيه في الأصل. يمكن للخدمات في النطاق البعيد إختيار ما إذا كانت سيتم تكريم بيانات الاعتماد هذه، وفقا لدرجة الأمان المطلوبة ومستوى الثقة في النطاق الذي قام بمصادقة المستخدم في البداية.

من أجل إجراء مصادقة عبر النطاق، من الضروري أن يقوم المسؤولون في كل زوج من العوالم بتحديد مفتاح ليتم مشاركته بين العوالم الخاصة بهم. ويمكن بعد ذلك لمستخدم في النطاق المحلي أن يطلب تذكرة لمنح التذاكر من خادم المصادقة المحلي لخادم منح التذاكر في النطاق البعيد. وعندما تستخدم تلك التذكرة، يدرك الخادم الذي يمنح التذاكر عن بعد أن الطلب ليس من مجاله الخاص، ويستخدم المفتاح الذي سبق تبادله لفك تشفير التذكرة التي تمنح التذاكر. ثم يصدر تذكرة كما تفعل عادة، باستثناء أن حقل النطاق الخاص بالعميل يحتوي على اسم النطاق الذي تم مصادقة العميل فيه في الأصل.

ويمكن توسيع هذا النهج بحيث يسمح للمرء بتوثيق نفسه من خلال سلسلة من المجالات حتى يصل إلى النطاق مع الخدمة المطلوبة. ولكن من أجل القيام بذلك، سيكون من الضروري تسجيل المسار بأكمله الذي تم إتخاذه، وليس فقط اسم النطاق الأولي الذي تم مصادقة المستخدم فيه. في مثل هذه الحالة، كل ما يعرفه الخادم هو أن A يقول أن B يقول أن المستخدم هو كذا وكذا. لا يمكن الوثوق بهذه الجملة إلا إذا كان كل شخص على المسار موثوقا به أيضا.

مشاكل Kerberos ومشاكل مفتوحة

هناك عدد من المشاكل والمشاكل المفتوحة المرتبطة بآلية مصادقة Kerberos. ومن بين هذه المشكلات كيفية تحديد العمر الصحيح للتذكرة وكيفية السماح للوكلاء وكيفية ضمان سلامة محطة العمل.

ومسألة مدة بقاء التذكرة هي مسألة إختيار المقايضة المناسبة بين الأمن والراحة. إذا كانت مدة صلاحية التذكرة طويلة، إذا سرقت التذكرة ومفتاح الجلسة المرتبط بها أو في غير موضعها، يمكن إستخدامهما لفترة أطول من الوقت. يمكن سرقة هذه المعلومات إذا نسي المستخدم تسجيل الخروج من محطة عمل عامة. وبدلا من ذلك، إذا تمت مصادقة مستخدم ما على نظام يسمح بالعديد من المستخدمين، فقد يتمكن مستخدم آخر لديه حق الوصول إلى الجذر من العثور على المعلومات اللازمة لاستخدام التذاكر المسروقة. المشكلة مع اعطاء تذكرة مدة قصيرة، هو انه عندما تنتهي، فان المستخدم سيضطر إلى الحصول على واحدة جديدة التي تتطلب من المستخدم إدخال كلمة مرة أخرى.

مشكلة مفتوحة هي مشكلة الوكيل. كيف يمكن لمستخدم مصدق أن يسمح للخادم بالحصول على خدمات شبكة أخرى نيابة عنه؟ والمثال الذي سيكون فيه هذا الأمر مهما هو إستخدام خدمة ستحصل على الوصول إلى الملفات المحمية مباشرة من خادم الملفات. مثال آخر على هذه المشكلة هو ما نسميه إعادة توجيه المصادقة. إذا قام المستخدم بتسجيل الدخول إلى محطة عمل وتسجيل الدخول إلى مضيف بعيد، فسيكون من الرائع إذا كان المستخدم لديه حق

الوصول إلى نفس الخدمات المتوفرة محليا، أثناء تشغيل برنامج على المضيف البعيد. وما يجعل هذا الأمر صعبا هو أن المستخدم قد لا يثق بالمضيف البعيد، وبالتالي فإن إعادة توجيه المصادقة غير مرغوب فيها في جميع الحالات. ليس لدينا حاليا حل لهذه المشكلة.

وهناك مشكلة أخرى، وهي مهمة في بيئة أثينا، وهي كيفية ضمان سلامة البرامج التي تعمل على محطة عمل. لا يمثل هذا مشكلة كبيرة بمحطات العمل الخاصة نظرا لأن المستخدم الذي سيستخدمه يتحكم فيه. ومع ذلك، في محطات العمل العامة، قد يأتي شخص ما ويقوم بتعديل برنامج تسجيل الدخول لحفظ كلمة مرور المستخدم. إن الحل الوحيد المتاح حاليا في بيئتنا هو جعل تعديل البرامج التي تعمل على محطات العمل العامة صعبا على الناس. يتطلب الحل الأفضل عدم ترك مفتاح المستخدم أبدا لنظام يعرف المستخدم أنه يمكن الوثوق به. وإحدى الطرق التي يمكن بها القيام بذلك هي حيازة المستخدم لبطاقة ذكية قادرة على القيام بالتشفير المطلوب في بروتوكول المصادقة.

حالة Kerberos

وبدأ إنتاج نسخة أولية من كيربروس في أيلول/سبتمبر 1986. ومنذ يناير/كانون الثاني من عام 1987، كانت شركة Kerberos هي الوسيلة الوحيدة للمصادقة على مستخدمي مشروع Athena البالغ عددهم 5000 مستخدم، و 650 محطة عمل، و 65 خادما. بالإضافة إلى ذلك، فإنه يتم الآن إستخدام Kerberos بدلا من ملفات .rhosts للتحكم في الوصول في العديد من أنظمة Athena.

إقرارات Kerberos

في مستهل الأمر، صمم كيبريوس بواسطة ستيف ميلر و كليفورد نيومان بالاستعانة باقتراحات من جيف شيللر وجيري سالتزر. ومنذ ذلك الحين، اشترك أشخاص آخرون كثيرون في المشروع. من بينهم جيم أسبنس، بوب بالدوين، جون باربا، ريتشارد باش، جيم بلوم، بيل برااينت، مارك كولان، روب فرينش، دان جير، جون كول، جون كوبياتوفيتش، بوب مككي، براين ميرفي، جون أوستلوند كين راييرن، كريس ريد، جون روتشلس، مايك شانزر، بيل سومرفيلد، تيد تاسو، وين تريسي، وستان زاناروتي.

ونحن ممتنون لدانا غير، وكاثي ليبن، وجوش لوبار، وكين راييرن، وجيري سالتزر، وإد شتاينر، وروبرت فان رينسي، ووين تريسي الذي حسنت اقتراحاته مسودات سابقة لهذه الورقة.

"Jedlinsky، J.T. Kohl، and W.E. Sommerfield، "The Zever Notification System"، في وقائع مؤتمرات أوسينكس (Winter، 1988).

السيد روزنشتاين، د. إ. جير، و ب. ج. ليفين، في جلسات مؤتمر يوسينيكس (شتاء، 1988).

ر. ساندبرغ، د. غولدبرغ، س. كليمان، د. والش، و ب. ليون، "تصميم وتنفيذ نظام ملفات شبكة صن"، في وقائع مؤتمر يوسينيكس (الصيف، 1985).

الملحق: تطبيق Kerberos على نظام ملفات الشبكة (NFS) من SUN

يتمثل أحد المكونات الرئيسية لنظام محطة العمل Project Athena في الربط بين محطة العمل الخاصة بالمستخدم ووحدة تخزين الملفات الخاصة به (الدليل الرئيسي). توجد جميع وحدات التخزين الخاصة على مجموعة من أجهزة الكمبيوتر (المعروفة حاليا باسم VAX 11/750s) المخصصة لهذا الغرض. وهذا يتيح لنا تقديم خدمات على محطات عمل UNIX المتاحة للجمهور. عندما يقوم المستخدم بتسجيل الدخول إلى واحدة من محطات العمل المتاحة للجمهور، بدلا من ذلك التحقق من اسمه وكلمة المرور الخاصة به مقابل ملف كلمة مرور مقيم محليا، نستخدم Kerberos لتحديد أصالتها. يطلب برنامج تسجيل الدخول اسم مستخدم (كما هو الحال في أي نظام UNIX). يتم إستخدام اسم المستخدم هذا لجلب تذكرة منح تذكرة ل Kerberos. يستخدم برنامج تسجيل الدخول كلمة المرور لإنشاء مفتاح DES لفك تشفير التذكرة. في حالة نجاح فك التشفير، يتم تحديد موقع الدليل الرئيسي للمستخدم من خلال مراجعة خدمة التسمية Hesiod ويتم تحميله عبر NFS. وبعد ذلك يقوم برنامج تسجيل الدخول بتحويل التحكم إلى Shell الخاص بالمستخدم، والذي يمكن بعد ذلك تشغيل ملفات التخصيص التقليدية لكل مستخدم نظرا لأن الدليل الرئيسي الآن "مرفق" بمحطة العمل. كما يتم إستخدام خدمة Hesiod لإنشاء إدخال في ملف كلمة المرور المحلي. (هذا لصالح

البرامج التي تبحث عن المعلومات في /etc/passwd.)

من بين خيارات عديدة لتقديم خدمة الملفات عن بعد، اخترنا نظام ملفات الشبكة ل Sun. لكن هذا النظام لا يتلاءم مع إحتياجاتنا بشكل حاسم. تفترض NFS أن جميع محطات العمل تقع في فئتين (كما هو معروض من وجهة نظر خادم الملفات): موثوق بها وغير موثوق بها. يتعذر على الأنظمة غير الموثوق بها الوصول إلى أي ملفات على الإطلاق، يمكن للثقة الوصول إليها. الأنظمة الموثوقة موثوق بها تماما. من المفترض أن النظام الموثوق تتم إدارته بواسطة إدارة سهلة. وعلى وجه الخصوص، يمكن التنكر من محطة العمل الموثوق بها كأي مستخدم صالح لنظام خدمة الملفات وبالتالي الحصول على إمكانية الوصول إلى كل ملف تقريبا على النظام. (يتم إستثناء الملفات المملوكة ل "root" فقط.)

في بيئتنا، تكون إدارة محطة العمل (بالمعنى التقليدي لإدارة نظام UNIX) في أيدي المستخدم الذي يستخدمها حاليا. فنحن لا نخفي كلمة المرور الجذر على محطات العمل الخاصة بنا، حيث أننا ندرك أن المستخدم غير المألوف حقا يمكن أن ينشق بمجرد أنه يجلس في نفس المكان المادي الذي يجلس فيه الجهاز ويتمتع بإمكانية الوصول إلى جميع وظائف وحدة التحكم. لذلك لا يمكننا أن نثق حقا بمحطات عملنا في تفسير نظام الضمان الوطني للثقة. للسماح بالتحكم بالوصول السليم في بيئتنا كان علينا إجراء بعض التعديلات على برمجيات NFS الأساسية وإدماج Kerberos في النظام.

نظام ملفات الشبكة (NFS) غير المعدل ل Kerberos

وفي تنفيذ نظام نظام الحسابات القومية الذي بدأنا به (من جامعة ويسكنسن)، قدمت المصادقة في شكل جزء من البيانات مدرج في كل طلب من طلبات نظام الأمن الوطني (يسمى "بيانات الاعتماد" في مصطلحات نظام ملفات الشبكة). تحتوي بيانات الاعتماد هذه على معلومات حول معرف المستخدم الفريد (UID) الخاص بالطالب وقائمة بمعرفات المجموعة (GIDs) الخاصة بعضوية الطالب. ثم يتم إستخدام هذه المعلومات من قبل خادم NFS لفحص الوصول. الفرق بين محطة العمل الموثوق بها وغير الموثوق بها هو ما إذا كانت بيانات الاعتماد الخاصة بها مقبولة من قبل خادم NFS أم لا.

NFS المعدل ل Kerberos

في بيئتنا، يجب أن تقبل خوادم NFS بيانات الاعتماد من محطة عمل إذا كانت بيانات الاعتماد تشير إلى UID الخاص بمستخدم محطة العمل وليس أي معرف آخر.

ويتمثل أحد الحلول الواضحة في تغيير طبيعة وثائق الإعتماد من مجرد مؤشرات لمعرف المستخدم و GID إلى بيانات مصدق عليها كاملة ل Kerberos. بيد أنه ستفرض في حالة اعتماد هذا الحل عقوبة كبيرة على الأداء. يتم تبادل بيانات الاعتماد في كل عملية NFS بما في ذلك كافة أنشطة قراءة القرص والكتابة. ومن شأن تضمين مصادقة Kerberos على كل معاملة من معاملات الأقراص إضافة عدد عادل من عمليات التشفير الكاملة (التي يتم إجراؤها في البرنامج) لكل معاملة، ووفقا لحساباتنا الخاصة بالمغلفات، فإنها توفر أداء غير مقبول. (قد يتطلب أيضا وضع موجهات مكتبة Kerberos في مساحة عنوان kernel.)

كنا بحاجة لنهج هجين، مشار إليه أسفله. تتمثل الفكرة الأساسية في الحصول على بيانات اعتماد خريطة خادم NFS مستلمة من محطات عمل العملاء، لبيانات اعتماد صالحة (وربما مختلفة) على نظام الخادم. يتم تنفيذ هذا التعيين في نواة الخادم في كل معاملة من معاملات NFS ويتم إعداده في وقت "التحميل" بواسطة عملية على مستوى المستخدم تقوم بالانخراط في المصادقة المعتدلة ل Kerberos قبل إنشاء تعيين بيانات اعتماد صالح ل kernel.

لتنفيذ ذلك، قمنا بإضافة اتصال نظام جديد إلى kernel (مطلوب فقط على أنظمة الخوادم وليس على أنظمة العملاء) الذي يوفر إمكانية التحكم في وظيفة التعيين التي تقوم بتعيين بيانات الاعتماد الواردة من محطات العمل العميلة إلى بيانات الاعتماد الصالحة للاستخدام على الخادم (إن وجدت). تقوم دالة التعيين الأساسية بتعيين المجموعة:

```
<CLIENT-IP-ADDRESS, UID-ON-CLIENT>
```

إلى بيانات اعتماد NFS صالحة على نظام الخادم. يتم إستخراج عنوان IP الخاص بالعميل من حزمة طلب NFS التي يتم توفيرها بواسطة نظام العميل. ملاحظة: تم تجاهل كافة المعلومات الواردة في بيانات الاعتماد التي أنشأها العميل باستثناء UID-on-Client.

في حالة عدم وجود تعيين، يتفاعل الخادم بإحدى الطريقتين، وفقا لتكوينه. في التكوين المألوف الخاص بنا، نقوم بإفتراض الطلبات التي لا يمكن تعيينها في بيانات الاعتماد للمستخدم "لا أحد" الذي ليس له حق الوصول المميز وله معرف فريد. تقوم الخوادم غير المألوفة بإرجاع خطأ وصول NFS عندما لا يمكن العثور على تعيين صحيح لبيانات اعتماد NFS الواردة.

يتم إستخدام إستدعاء النظام الجديد لإضافة إدخالات من الخريطة المقيمة ل kernel وحذفها. كما توفر إمكانية مسح جميع الإدخالات التي تخطط لمعرف فريد معين على نظام الخادم، أو مسح جميع الإدخالات من عنوان IP لعميل معين.

قمنا بتعديل البرنامج الخفي للتحميل (الذي يعالج طلبات تحميل NFS على أنظمة الخادم) لقبول نوع معاملة جديد، وهو طلب تعيين مصادقة Kerberos. وبشكل أساسي، وكجزء من عملية التركيب، يوفر نظام العميل مصدقا ل Kerberos مع إشارة إلى UID-on-client الخاص به (المشفر في مصدق Kerberos) على محطة العمل. يقوم البرنامج الخفي الخاص بتحميل الخادم بتحويل اسم Kerberos الأساسي إلى اسم مستخدم محلي. بعد ذلك يتم البحث عن اسم المستخدم هذا في ملف خاص للحصول على UID الخاص بالمستخدم وقائمة GIDs. للكفاءة، هذا الملف هو ملف قاعدة بيانات ndbm مع اسم المستخدم كمفتاح. من هذه المعلومات، يتم إنشاء بيانات اعتماد NFS وتسليمها إلى kernel كتعيين صحيح لمجموعة <CLIENT-IP-ADDRESS و CLIENT-UID> الخاصة بهذا الطلب.

عند إلغاء التحميل، يتم إرسال طلب إلى الخادم المركب لإزالة التعيين الذي تمت إضافته مسبقا من kernel. من الممكن أيضا إرسال طلب عند تسجيل الخروج لإبطال كافة التعيينات الخاصة بالمستخدم الحالي على الخادم المعني، ومن ثم تنظيف أية تعيينات متبقية موجودة (على الرغم من أنها لا يجب أن تكون كذلك) قبل أن يتم توفير محطة العمل للمستخدم التالي.

تأثيرات أمان Kerberos الخاصة ب NFS المعدل

هذا التطبيق غير آمن تماما. بالنسبة للمبتدئين، لا تزال بيانات المستخدم يتم إرسالها عبر الشبكة بشكل غير مشفر، وبالتالي يمكن اعتراضه. تعتمد المصادقة منخفضة المستوى لكل معاملة على زوج <CLIENT-IP-ADDRESS و CLIENT-UID> الذي تم توفيره غير مشفر في حزمة الطلب. ويمكن تزوير هذه المعلومات وبالتالي تعريض الأمن للخطر. ومع ذلك، تجدر الإشارة إلى أنه في الوقت الذي يستخدم فيه المستخدم ملفاته بشكل نشط (أي أثناء تسجيل الدخول) فقط تكون التعيينات الصحيحة في مكانها، وبالتالي يقتصر هذا الشكل من الهجوم على الوقت الذي يتم فيه تسجيل دخول المستخدم. في حالة عدم تسجيل دخول المستخدم، فلن يسمح أي مقدار من تزييف عنوان IP بالوصول غير المصرح به إلى ملفاته.

مراجع Kerberos

1. S.P. Miller و B.C. Neuman و J.I. Schiller و J.H. Saltzer، القسم E.2.1: نظام Kerberos للمصادقة والإذن، 21) M.I.T. Project Athena، Cambridge، Massachusetts كانون الأول/ديسمبر 1987).
2. R.P. Parmelee، "Computing in High Education: The Athena و E. Balkovich، S.R. Lerman Experience" Communications of ACM، vol. 28(11)، pp. 1214-1224، ACM (نوفمبر، 1985).
3. م. نيدهام و م. د. شرودر، "إستخدام التشفير للمصادقة في شبكات كبيرة من أجهزة الكمبيوتر"، مراسلات ACM، المجلد 21(12)، الصفحات 993-999 (كانون الأول/ديسمبر 1978).
4. V.L. Voydock و S.T. Kent، "آليات الأمن في بروتوكولات الشبكة الرفيعة المستوى"، الدراسات الاستقصائية الحاسوبية، المجلد 15(2)، ACM (حزيران/يونيه 1983).
5. المكتب الوطني للمعايير، "معيار تشفير البيانات"، منشور المعايير الاتحادية لتجهيز المعلومات 46، مكتب الطباعة الحكومي، واشنطن، العاصمة (1977).
6. SP Dyer، "Hesiod"، في مداولات مؤتمر يوسنكس (شتاء، 1988).
7. برينت، البرنامج التعليمي لمبرمج كيربيروس، مشروع MIT Athena (قيد الإعداد).
8. برينت، دليل مسؤول Kerberos، مشروع MIT Athena (قيد الإعداد).
9. G.W. Treese، "Berkeley Unix على 1000 محطة عمل: Athena تتغير إلى 4.3 BSD"، في وقائع مؤتمرات Usenix (شتاء، 1988).

10. J.T. Kohl، R.S. French، D.C. Jedlinsky، M.W. Eichin، C.A. DellaFera، و W.E. Sommerfeld، "نظام Zephyr Notification"، في وقائع مؤتمر Usenix (شتاء، 1988).
11. السيد روزنشتاين، د. إ. جير، و ب. ج. ليفين، في جلسات مؤتمر يوسينيكس (شتاء، 1988).
12. ر. ساندبرغ، د. غولدبرغ، س. كليمان، د. والش، و ب. ليون، "تصميم وتنفيذ نظام ملفات شبكة صن"، في وقائع مؤتمر يوسينيكس (الصيف، 1985).

معلومات ذات صلة

- صفحة دعم Kerberos
- 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).